

THE DISTRIBUTION OF FACTORIZATION PATTERNS ON LINEAR FAMILIES OF POLYNOMIALS OVER A FINITE FIELD

EDA CESARATTO^{1,2}, GUILLERMO MATERA^{1,2}, MARIANA PÉREZ¹,

ABSTRACT. We obtain estimates on the number $|\mathcal{A}_\lambda|$ of elements on a linear family \mathcal{A} of monic polynomials of $\mathbb{F}_q[T]$ of degree n having factorization pattern $\lambda := 1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$. We show that $|\mathcal{A}_\lambda| = \mathcal{T}(\lambda) q^{n-m} + \mathcal{O}(q^{n-m-1/2})$, where $\mathcal{T}(\lambda)$ is the proportion of elements of the symmetric group of n elements with cycle pattern λ and m is the codimension of \mathcal{A} . Furthermore, if the family \mathcal{A} under consideration is “sparse”, then $|\mathcal{A}_\lambda| = \mathcal{T}(\lambda) q^{n-m} + \mathcal{O}(q^{n-m-1})$. Our estimates hold for fields \mathbb{F}_q of characteristic greater than 2. We provide explicit upper bounds for the constants underlying the \mathcal{O} -notation in terms of λ and \mathcal{A} with “good” behavior. Our approach reduces the question to estimate the number of \mathbb{F}_q -rational points of certain families of complete intersections defined over \mathbb{F}_q . Such complete intersections are defined by polynomials which are invariant under the action of the symmetric group of permutations of the coordinates. This allows us to obtain critical information concerning their singular locus, from which precise estimates on their number of \mathbb{F}_q -rational points are established.

1. INTRODUCTION

Let \mathbb{F}_q be the finite field of $q := p^s$ elements, where p is a prime number, and let $\overline{\mathbb{F}_q}$ denote its algebraic closure. Let T be an indeterminate over $\overline{\mathbb{F}_q}$ and $\mathbb{F}_q[T]$ the set of polynomials in T with coefficients in \mathbb{F}_q . Let n be a positive integer and $\mathcal{P} := \mathcal{P}_n$ the set of all monic polynomials in $\mathbb{F}_q[T]$ of degree n . Let $\lambda_1, \dots, \lambda_n$ be nonnegative integers such that

$$\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = n.$$

We denote by \mathcal{P}_λ the set of elements \mathcal{P} with factorization pattern $\lambda := 1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$, namely the elements $f \in \mathcal{P}$ which have exactly λ_i monic irreducible factors over \mathbb{F}_q of degree i (counted with multiplicity) for $1 \leq i \leq n$. We shall further use the notation $\mathcal{S}_\lambda := \mathcal{S} \cap \mathcal{P}_\lambda$ for any subset $\mathcal{S} \subset \mathcal{P}$.

In [Coh70] it was noted that the proportion of elements of \mathcal{P}_λ in \mathcal{P} is roughly the proportion $\mathcal{T}(\lambda)$ of permutations with cycle pattern λ in the n th symmetric group \mathbb{S}_n . More precisely, it was shown that

$$(1.1) \quad |\mathcal{P}_\lambda| = \mathcal{T}(\lambda) q^n + \mathcal{O}(q^{n-\frac{1}{2}}),$$

where the constant underlying the \mathcal{O} -notation depends only on λ . A permutation of \mathbb{S}_n has cycle pattern λ if it has exactly λ_i cycles of length i for $1 \leq i \leq n$.

Date: September 6, 2014.

1991 Mathematics Subject Classification. 12E05, 11T06, 12E20, 11G25, 14G05, 14G15, 14B05.

Key words and phrases. Finite fields, factorization patterns, symmetric polynomials, singular complete intersections, rational points.

The authors were partially supported by the grants PIP CONICET 11220090100421, UNGS 30/3180 and STIC-AmSud 13STIC-02 “Dynalco”.

Observe that

$$\mathcal{T}(\boldsymbol{\lambda}) := \frac{1}{w(\boldsymbol{\lambda})}, \quad w(\boldsymbol{\lambda}) := 1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} \lambda_1! \lambda_2! \dots \lambda_n!.$$

In particular, $n!/w(\boldsymbol{\lambda})$ is the number of permutations in \mathbb{S}_n with cycle pattern $\boldsymbol{\lambda}$.

Furthermore, in [Coh72] a subset $\mathcal{S} \subset \mathcal{P}_{\boldsymbol{\lambda}}$ is called *uniformly distributed* if the proportion $|\mathcal{S}_{\boldsymbol{\lambda}}|/|\mathcal{S}|$ is roughly $\mathcal{T}(\boldsymbol{\lambda})$ for every factorization pattern $\boldsymbol{\lambda}$. The main result of this paper ([Coh72, Theorem 3]) provides a criterion for a linear family of polynomials of \mathcal{P} to be uniformly distributed in the sense above. As a particular case we have the classical case of polynomials with prescribed coefficients, where simpler conditions are obtained (see [Coh72, Theorem 1]; see also [Ste87]).

A difficulty with [Coh72, Theorem 3] is that the hypotheses for a linear family of \mathcal{P} to be uniformly distributed seem complicated and not easy to verify. In fact, in [GHP99] it is asserted that “more work need to be done to simplify Cohen’s conditions”. A second concern is that [Coh72, Theorem 3] imposes restrictions on the characteristic p of \mathbb{F}_q which may inhibit its application to fields of small characteristic. Finally, we are also interested in finding explicit estimates, namely an explicit admissible expression for the constant underlying (1.1).

In this paper we consider the linear families in \mathcal{P} that we now describe. Let m, r be positive integers with $3 \leq r \leq n - m$, let A_r, \dots, A_{n-1} be indeterminates over \mathbb{F}_q , and let be given linear forms L_1, \dots, L_m of $\mathbb{F}_q[A_r, \dots, A_{n-1}]$ which are linearly independent and $\boldsymbol{\alpha} := (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m$. Set $\boldsymbol{L} := (L_1, \dots, L_m)$ and define $\mathcal{A} := \mathcal{A}(\boldsymbol{L}, \boldsymbol{\alpha})$ as

$$(1.2) \quad \mathcal{A} := \{T^n + a_{n-1}T^{n-1} + \dots + a_0 \in \mathbb{F}_q[T] : \boldsymbol{L}(a_r, \dots, a_{n-1}) + \boldsymbol{\alpha} = \mathbf{0}\}.$$

Our main results assert that any such family \mathcal{A} is uniformly distributed. More precisely, we have the following result.

Theorem 1.1. *Let $\mathcal{A}_{\boldsymbol{\lambda}} := \mathcal{A} \cap \mathcal{P}_{\boldsymbol{\lambda}}$. If $p > 2$, $q > n$ and $3 \leq r \leq n - m$, then*

$$(1.3) \quad \left| |\mathcal{A}_{\boldsymbol{\lambda}}| - \mathcal{T}(\boldsymbol{\lambda}) q^{n-m} \right| \leq q^{n-m-1} (2 \mathcal{T}(\boldsymbol{\lambda}) D_{\boldsymbol{L}} \delta_{\boldsymbol{L}} q^{\frac{1}{2}} + 19 \mathcal{T}(\boldsymbol{\lambda}) D_{\boldsymbol{L}}^2 \delta_{\boldsymbol{L}}^2 + n(n-1)).$$

On the other hand, if $q > n$ and $m + 2 \leq r \leq n - m$, then

$$(1.4) \quad \left| |\mathcal{A}_{\boldsymbol{\lambda}}| - \mathcal{T}(\boldsymbol{\lambda}) q^{n-m} \right| \leq q^{n-m-1} (21 \mathcal{T}(\boldsymbol{\lambda}) D_{\boldsymbol{L}}^3 \delta_{\boldsymbol{L}}^2 + n(n-1)).$$

Here $\delta_{\boldsymbol{L}}$ and $D_{\boldsymbol{L}}$ are certain explicit discrete invariants associated to the linear variety \boldsymbol{L} under consideration. We have the worst-case upper bounds $\delta_{\boldsymbol{L}} \leq (n-3)!/(n-m-3)!$ and $D_{\boldsymbol{L}} \leq m(n-2)$.

It might be worthwhile to explicitly state what Theorem 1.1 asserts when the family \mathcal{A} of (1.2) consists of the polynomials of \mathcal{P} with certain prescribed coefficients. More precisely, given $0 < i_1 < i_2 < \dots < i_m \leq n$ and $\boldsymbol{\alpha} := (\alpha_{i_1}, \dots, \alpha_{i_m}) \in \mathbb{F}_q^m$, set $\mathcal{I} := \{i_1, \dots, i_m\}$ and

$$\mathcal{A}^m := \mathcal{A}^m(\mathcal{I}, \boldsymbol{\alpha}) := \{T^n + a_1 T^{n-1} + \dots + a_n \in \mathbb{F}_q[T] : a_{i_j} = \alpha_{i_j} \ (1 \leq j \leq m)\}.$$

Let $\delta_{\mathcal{I}} := i_1 \dots i_m$ and $D_{\mathcal{I}} := \sum_{j=1}^m (i_j - 1)$. We have the following result.

Theorem 1.2. *If $p > 2$, $q > n$ and $i_m \leq n - 3$, then*

$$\left| |\mathcal{A}_{\boldsymbol{\lambda}}^m| - \mathcal{T}(\boldsymbol{\lambda}) q^{n-m} \right| \leq q^{n-m-1} (2 \mathcal{T}(\boldsymbol{\lambda}) D_{\mathcal{I}} \delta_{\mathcal{I}} q^{\frac{1}{2}} + 19 \mathcal{T}(\boldsymbol{\lambda}) D_{\mathcal{I}}^2 \delta_{\mathcal{I}}^2 + n(n-1)).$$

On the other hand, for $q > n$ and $i_m \leq n - m - 2$, we have

$$\left| |\mathcal{A}_{\boldsymbol{\lambda}}^m| - \mathcal{T}(\boldsymbol{\lambda}) q^{n-m} \right| \leq q^{n-m-1} (21 \mathcal{T}(\boldsymbol{\lambda}) D_{\mathcal{I}}^3 \delta_{\mathcal{I}}^2 + n(n-1)).$$

Theorem 1.1 strengthens (1.1) in several aspects. First of all, the hypotheses on the linear families \mathcal{A} in the statement of Theorem 1.1 are relatively wide and easy to verify. On the other hand, our results are valid either for $p > 2$ or without any restriction on the characteristic p of \mathbb{F}_q , while (1.1) requires that p is large enough. A third aspect it is worth mentioning is that (1.4) shows that $|\mathcal{A}_\lambda| = \mathcal{T}(\lambda) q^{n-m} + \mathcal{O}(q^{n-m-1})$, while (1.1) only asserts that $|\mathcal{A}_\lambda| = \mathcal{T}(\lambda) q^{n-m} + \mathcal{O}(q^{n-m-\frac{1}{2}})$. Finally, both (1.3) and (1.4) provide explicit expressions for the constants underlying the \mathcal{O} -notation in (1.1) with a good behavior.

In order to prove Theorem 1.1, we express the number $|\mathcal{A}_\lambda|$ of polynomials in \mathcal{A} with factorization pattern λ in terms of the number of \mathbb{F}_q -rational solutions with pairwise-distinct coordinates of a system $\{R_1 = 0, \dots, R_m = 0\}$, where R_1, \dots, R_m are certain polynomials in $\mathbb{F}_q[X_1, \dots, X_n]$. A critical point for our approach is that, up to a linear change of coordinates, R_1, \dots, R_m are symmetric polynomials, namely invariant under any permutation of X_1, \dots, X_n . More precisely, we prove that each R_j can be expressed as a polynomial in the first $n - r$ elementary symmetric polynomials of $\mathbb{F}_q[X_1, \dots, X_n]$ (Corollary 2.4). This allows us to establish a number of facts concerning the geometry of the set V of solutions of such a polynomial system (see, e.g., Theorems 3.7, 3.11 and 5.1 and Corollary 5.2). Combining these results with estimates on the number of \mathbb{F}_q -rational points of singular complete intersections of [CMP12a], we obtain our main results (Theorems 4.2 and 5.4).

Our methodology differs significantly from that employed in [Coh70] and [Coh72], as we express $|\mathcal{A}_\lambda|$ in terms of the number of \mathbb{F}_q -rational points of certain singular complete intersections defined over \mathbb{F}_q . In [GHP99, Problem 2.2], the authors ask for estimates on the number of elements of \mathcal{P} , with a given factorization pattern, lying in nonlinear families of polynomials parameterized by an affine variety defined over \mathbb{F}_q . As a consequence of general results by [CvM92] and [FHJ94], it is known that $|\mathcal{A}_\lambda| = \mathcal{O}(q^r)$, where r is the dimension of the parameterizing affine variety under consideration. Nevertheless, very little is known on the asymptotic behavior of $|\mathcal{A}_\lambda|$ as a power of q and of the size of the constant underlying the \mathcal{O} -notation. We think that our methods may be extended to deal with this more general case, at least for certain classes of parameterizing affine varieties.

2. FACTORIZATION PATTERNS AND ROOTS

As before, let n be a positive integer with $q > n$ and let \mathcal{P} be the set of monic polynomials of $\mathbb{F}_q[T]$ of degree n . Let $\mathcal{A} \subset \mathcal{P}$ be the linear family defined in (1.2) and $\lambda := 1^{\lambda_1} \dots n^{\lambda_n}$ a factorization pattern. In this section we show that the number $|\mathcal{A}_\lambda|$ can be expressed in terms of the number of common \mathbb{F}_q -rational zeros of certain polynomials $R_1, \dots, R_m \in \mathbb{F}_q[X_1, \dots, X_n]$.

For this purpose, let f be an arbitrary element of \mathcal{P} and let $g \in \mathbb{F}_q[T]$ be a monic irreducible factor of f of degree i . Then g is the minimal polynomial of a root α of f with $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^i}$. Denote by \mathbb{G}_i the Galois group $\text{Gal}(\mathbb{F}_{q^i}, \mathbb{F}_q)$ of \mathbb{F}_{q^i} over \mathbb{F}_q . Then we may express g in the following way:

$$g = \prod_{\sigma \in \mathbb{G}_i} (T - \sigma(\alpha)).$$

Hence, each irreducible factor g of f is uniquely determined by a root α of f (and its orbit under the action of the Galois group of $\overline{\mathbb{F}_q}$ over \mathbb{F}_q), and this root belongs to a field extension of \mathbb{F}_q of degree $\deg g$. Now, for a polynomial $f \in \mathcal{P}_\lambda$, there are λ_1

roots of f in \mathbb{F}_q , say $\alpha_1, \dots, \alpha_{\lambda_1}$ (counted with multiplicity), which are associated with the irreducible factors of f in $\mathbb{F}_q[T]$ of degree 1; it is also possible to choose λ_2 roots of f in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ (counted with multiplicity), say $\alpha_{\lambda_1+1}, \dots, \alpha_{\lambda_1+\lambda_2}$, which are associated with the λ_2 irreducible factors of f of degree 2, and so on. From now on we shall assume that a choice of $\lambda_1 + \dots + \lambda_n$ roots $\alpha_1, \dots, \alpha_{\lambda_1+\dots+\lambda_n}$ of f in $\overline{\mathbb{F}_q}$ is made in such a way that each monic irreducible factor of f in $\mathbb{F}_q[T]$ is associated with one and only one of these roots.

Our aim is to express the factorization of f into irreducible factors in $\mathbb{F}_q[T]$ in terms of the coordinates of the chosen $\lambda_1 + \dots + \lambda_n$ roots of f with respect to suitable bases of the corresponding extensions $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^i}$ as \mathbb{F}_q -vector spaces. For this purpose, we express the root associated with each irreducible factor of f of degree i in a normal basis Θ_i of the field extension $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^i}$.

Let $\theta_i \in \mathbb{F}_{q^i}$ be a normal element and let Θ_i be the normal basis of $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^i}$ generated by θ_i , namely

$$\Theta_i = \left\{ \theta_i, \dots, \theta_i^{q^{i-1}} \right\}.$$

Observe that the Galois group \mathbb{G}_i is cyclic and the Frobenius map $\sigma : \mathbb{F}_{q^i} \rightarrow \mathbb{F}_{q^i}$, $\sigma(x) := x^q$ is a generator of \mathbb{G}_i . Thus, the coordinates in the basis Θ_i of all the elements in the orbit of a root $\alpha_k \in \mathbb{F}_{q^i}$ of an irreducible factor of f of degree i are the cyclic permutations of the coordinates of α_k in the basis Θ_i .

The vector that gathers the coordinates of all the roots $\alpha_1, \dots, \alpha_{\lambda_1+\dots+\lambda_n}$ we have chosen to represent the irreducible factors of f in the normal bases $\Theta_1, \dots, \Theta_n$ is an element of \mathbb{F}_q^n , which is denoted by $\mathbf{x} := (x_1, \dots, x_n)$. Set

$$(2.1) \quad \ell_{i,j} := \sum_{k=1}^{i-1} k\lambda_k + (j-1)i$$

for $1 \leq j \leq \lambda_i$ and $1 \leq i \leq n$. Observe that the vector of coordinates of a root $\alpha_{\lambda_1+\dots+\lambda_{i-1}+j} \in \mathbb{F}_{q^i}$ is the sub-array $(x_{\ell_{i,j}+1}, \dots, x_{\ell_{i,j}+i})$ of \mathbf{x} . With this notation, the λ_i irreducible factors of f of degree i are the polynomials

$$(2.2) \quad g_{i,j} = \prod_{\sigma \in \mathbb{G}_i} \left(T - (x_{\ell_{i,j}+1}\sigma(\theta_i) + \dots + x_{\ell_{i,j}+i}\sigma(\theta_i^{q^{i-1}})) \right)$$

for $1 \leq j \leq \lambda_i$. In particular,

$$(2.3) \quad f = \prod_{i=1}^n \prod_{j=1}^{\lambda_i} g_{i,j}.$$

Let X_1, \dots, X_n be indeterminates over $\overline{\mathbb{F}_q}$, set $\mathbf{X} := (X_1, \dots, X_n)$ and consider the polynomial $G \in \mathbb{F}_q[\mathbf{X}, T]$ defined as

$$(2.4) \quad G := \prod_{i=1}^n \prod_{j=1}^{\lambda_i} G_{i,j}, \quad G_{i,j} := \prod_{\sigma \in \mathbb{G}_i} \left(T - (X_{\ell_{i,j}+1}\sigma(\theta_i) + \dots + X_{\ell_{i,j}+i}\sigma(\theta_i^{q^{i-1}})) \right),$$

where the $\ell_{i,j}$ are defined as in (2.1). Our previous arguments show that an element $f \in \mathcal{P}$ has factorization pattern $\boldsymbol{\lambda}$ if and only if there exists $\mathbf{x} \in \mathbb{F}_q^n$ with $f = G(\mathbf{x}, T)$.

Next we discuss how many elements $\mathbf{x} \in \mathbb{F}_q^n$ yield an arbitrary polynomial $f = G(\mathbf{x}, T) \in \mathcal{P}_{\boldsymbol{\lambda}}$. For $\alpha \in \mathbb{F}_{q^i}$, we have that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^i}$ if and only if its orbit under the action of the Galois group \mathbb{G}_i has exactly i elements. In particular, if α is expressed by its coordinate vector $\mathbf{x} \in \mathbb{F}_q^i$ in the normal basis Θ_i , then the coordinate vectors

of the elements of the orbit of α form a cycle of length i , because \mathbb{G}_i permutes cyclically the coordinates. As a consequence, there is a bijection between cycles of length i in \mathbb{F}_q^i and elements $\alpha \in \mathbb{F}_q^i$ with $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^i}$.

In this setting, the notion of an array of type λ will prove to be useful.

Definition 2.1. Let $\ell_{i,j}$ ($1 \leq i \leq n$, $1 \leq j \leq \lambda_i$) be defined as in (2.1). An element $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ is said to be of type λ if and only if each sub-array $\mathbf{x}_{i,j} := (x_{\ell_{i,j}+1}, \dots, x_{\ell_{i,j}+i})$ is a cycle of length i .

The next result relates \mathcal{P}_λ with the set of elements of \mathbb{F}_q^n of type λ .

Lemma 2.2. For any $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$, the polynomial $f := G(\mathbf{x}, T)$ has factorization pattern λ if and only if \mathbf{x} is of type λ . Furthermore, for each square-free polynomial $f \in \mathcal{P}_\lambda$ there are $w(\lambda) := \prod_{i=1}^n i^{\lambda_i} \lambda_i!$ different $\mathbf{x} \in \mathbb{F}_q^n$ with $f = G(\mathbf{x}, T)$.

Proof. Let $\Theta_1, \dots, \Theta_n$ be the normal bases introduced before. Each $\mathbf{x} \in \mathbb{F}_q^n$ is associated with a unique finite sequence of elements α_k ($1 \leq k \leq \lambda_1 + \dots + \lambda_n$) as follows: each $\alpha_{\lambda_1 + \dots + \lambda_{i-1} + j}$ with $1 \leq j \leq \lambda_i$ is the element of \mathbb{F}_{q^i} whose coordinate vector in the basis Θ_i is the sub-array $(x_{\ell_{i,j}+1}, \dots, x_{\ell_{i,j}+i})$ of \mathbf{x} .

Suppose that $G(\mathbf{x}, T)$ has factorization pattern λ for a given $\mathbf{x} \in \mathbb{F}_q^n$. Fix (i, j) with $1 \leq i \leq n$ and $1 \leq j \leq \lambda_i$. Then $G(\mathbf{x}, T)$ is factored as in (2.2)–(2.3), where each $g_{i,j} \in \mathbb{F}_q[T]$ is irreducible, and hence $\mathbb{F}_q(\alpha_{\lambda_1 + \dots + \lambda_{i-1} + j}) = \mathbb{F}_{q^i}$. We conclude that the sub-array $(x_{\ell_{i,j}+1}, \dots, x_{\ell_{i,j}+i})$ defining $\alpha_{\lambda_1 + \dots + \lambda_{i-1} + j}$ is a cycle of length i . This proves that \mathbf{x} is of type λ .

On the other hand, assume that we are given $\mathbf{x} \in \mathbb{F}_q^n$ of type λ and fix (i, j) with $1 \leq i \leq n$ and $1 \leq j \leq \lambda_i$. Then $\mathbb{F}_q(\alpha_{\lambda_1 + \dots + \lambda_{i-1} + j}) = \mathbb{F}_{q^i}$, because the sub-array $(x_{\ell_{i,j}+1}, \dots, x_{\ell_{i,j}+i})$ is a cycle of length i and thus the orbit of $\alpha_{\lambda_1 + \dots + \lambda_{i-1} + j}$ under the action of \mathbb{G}_i has i elements. This implies that the factor $g_{i,j}$ of $G(\mathbf{x}, T)$ defined as in (2.2) is irreducible of degree i . We deduce that $f := G(\mathbf{x}, T)$ has factorization pattern λ .

Furthermore, for $\mathbf{x} \in \mathbb{F}_q^n$ of type λ , the polynomial $f := G(\mathbf{x}, T) \in \mathcal{P}_\lambda$ is square-free if and only if all the roots $\alpha_{\lambda_1 + \dots + \lambda_{i-1} + j}$ with $1 \leq j \leq \lambda_i$ are pairwise-distinct, non-conjugated elements of \mathbb{F}_{q^i} . This implies that no cyclic permutation of a sub-array $(x_{\ell_{i,j}+1}, \dots, x_{\ell_{i,j}+i})$ with $1 \leq j \leq \lambda_i$ agrees with another cyclic permutation of another sub-array $(x_{\ell_{i,j'}+1}, \dots, x_{\ell_{i,j'}+i})$. As cyclic permutations of any of these sub-arrays and permutations of these sub-arrays yield elements of \mathbb{F}_q^n associated with the same polynomial f , we conclude that there are $w(\lambda) := \prod_{i=1}^n i^{\lambda_i} \lambda_i!$ different elements $\mathbf{x} \in \mathbb{F}_q^n$ with $f = G(\mathbf{x}, T)$. \square

2.1. G in terms of the elementary symmetric polynomials. Consider the polynomial G of (2.4) as an element of $\mathbb{F}_q[\mathbf{X}][T]$. We shall express the coefficients of G by means of the vector of linear forms $\mathbf{Y} := (Y_1, \dots, Y_n) \in \overline{\mathbb{F}_q}[\mathbf{X}]$ defined in the following way:

$$(2.5) \quad (Y_{\ell_{i,j}+1}, \dots, Y_{\ell_{i,j}+i})^t := A_i \cdot (X_{\ell_{i,j}+1}, \dots, X_{\ell_{i,j}+i})^t \quad (1 \leq j \leq \lambda_i, 1 \leq i \leq n),$$

where $A_i \in \mathbb{F}_q^{i \times i}$ is the matrix

$$A_i := \left(\sigma(\theta_i^{q^h}) \right)_{\sigma \in \mathbb{G}_i, 1 \leq h \leq i}.$$

According to (2.4), we may express the polynomial G as

$$G = \prod_{i=1}^n \prod_{j=1}^{\lambda_i} \prod_{k=1}^i (T - Y_{\ell_{i,j}+k}) = \prod_{k=1}^n (T - Y_k) = T^n + \sum_{k=1}^n (-1)^k (\Pi_k(\mathbf{Y})) T^{n-k},$$

where $\Pi_1(\mathbf{Y}), \dots, \Pi_n(\mathbf{Y})$ are the elementary symmetric polynomials of $\mathbb{F}_q[\mathbf{Y}]$. By the expression of G in (2.4) we deduce that G belongs to $\mathbb{F}_q[\mathbf{X}, T]$, which in particular implies that $\Pi_k(\mathbf{Y})$ belongs to $\mathbb{F}_q[\mathbf{X}]$ for $1 \leq k \leq n$. Combining these arguments with Lemma 2.2 we obtain the following result.

Lemma 2.3. *A polynomial $f := T^n + a_{n-1}T^{n-1} + \dots + a_0 \in \mathcal{P}$ has factorization pattern λ if and only if there exists $\mathbf{x} \in \mathbb{F}_q^n$ of type λ such that*

$$(2.6) \quad a_k = (-1)^{n-k} \Pi_{n-k}(\mathbf{Y}(\mathbf{x})) \quad (0 \leq k \leq n-1).$$

In particular, if f is square-free, then there are $w(\lambda)$ elements \mathbf{x} for which (2.6) holds.

An easy consequence of this result is that we may express the condition that an element of $\mathcal{A} := \mathcal{A}(\mathbf{L}, \alpha)$ has factorization pattern λ in terms of the elementary symmetric polynomials Π_1, \dots, Π_{n-r} of $\mathbb{F}_q[\mathbf{Y}]$.

Corollary 2.4. *A polynomial $f := T^n + a_{n-1}T^{n-1} + \dots + a_0 \in \mathcal{A}$ has factorization pattern λ if and only if there exists $\mathbf{x} \in \mathbb{F}_q^n$ of type λ such that*

$$(2.7) \quad L_j((-1)^{n-r} \Pi_{n-r}(\mathbf{Y}(\mathbf{x})), \dots, -\Pi_1(\mathbf{Y}(\mathbf{x}))) + \alpha_j = 0 \quad (1 \leq j \leq m).$$

In particular, if $f \in \mathcal{A}_\lambda$ is square-free, then there are $w(\lambda)$ elements \mathbf{x} for which (2.7) holds.

3. THE GEOMETRY OF THE SET OF ZEROS OF R_1, \dots, R_m

Let m, n and r be positive integers with $q > n$ and $3 \leq r \leq n - m$. Given a factorization pattern $\lambda := 1^{\lambda_1} \dots n^{\lambda_n}$, consider the family $\mathcal{A}_\lambda \subset \mathbb{F}_q[T]$ of monic polynomials of degree n having factorization pattern λ , where $\mathcal{A} \subset \mathcal{P}$ is the linear family defined in (1.2). In Corollary 2.4 we associate to \mathcal{A}_λ the following polynomials of $\mathbb{F}_q[\mathbf{X}] := \mathbb{F}_q[X_1, \dots, X_n]$:

$$(3.1) \quad R_j := R_j^\lambda := L_j((-1)^{n-r} \Pi_{n-r}(\mathbf{Y}(\mathbf{X})), \dots, -\Pi_1(\mathbf{Y}(\mathbf{X}))) + \alpha_j \quad (1 \leq j \leq m).$$

The set of common \mathbb{F}_q -rational zeros of R_1, \dots, R_m are relevant for our purposes.

Up to the linear change of coordinates defined by $\mathbf{Y} := (Y_1, \dots, Y_n)$, we may express each R_j as a linear polynomial in the first $n - r$ elementary symmetric polynomials Π_1, \dots, Π_{n-r} of $\mathbb{F}_q[\mathbf{Y}]$. More precisely, let Z_1, \dots, Z_{n-r} be new indeterminates over $\overline{\mathbb{F}_q}$. Then we have that

$$R_j = S_j(\Pi_1, \dots, \Pi_{n-r}) \quad (1 \leq j \leq m),$$

where $S_1, \dots, S_m \in \mathbb{F}_q[Z_1, \dots, Z_{n-r}]$ are elements of degree 1 whose homogeneous components of degree 1 are linearly independent in $\overline{\mathbb{F}_q}[Z_1, \dots, Z_{n-r}]$, namely the Jacobian matrix $(\partial S / \partial \mathbf{Z})$ of S_1, \dots, S_m with respect to $\mathbf{Z} := (Z_1, \dots, Z_{n-r})$ has full rank m .

In this section we obtain critical information on the geometry of the set of common zeros of the polynomials R_1, \dots, R_m that will allow us to establish estimates on their number of common \mathbb{F}_q -rational zeros.

3.1. Notions of algebraic geometry. Since our approach relies on tools of algebraic geometry, we briefly collect the basic definitions and facts that we need in the sequel. We use standard notions and notations of algebraic geometry, which can be found in, e.g., [Kun85, Sha94].

We denote by \mathbb{A}^n the affine n -dimensional space $\overline{\mathbb{F}}_q^n$ and by \mathbb{P}^n the projective n -dimensional space over $\overline{\mathbb{F}}_q^{n+1}$. Both spaces are endowed with their respective Zariski topologies, for which a closed set is the zero locus of polynomials of $\overline{\mathbb{F}}_q[X_1, \dots, X_n]$ or of homogeneous polynomials of $\overline{\mathbb{F}}_q[X_0, \dots, X_n]$. For $\mathbb{K} := \mathbb{F}_q$ or $\mathbb{K} := \overline{\mathbb{F}}_q$, we say that a subset $V \subset \mathbb{A}^n$ is an **affine \mathbb{K} -definable variety** (or simply **affine \mathbb{K} -variety**) if it is the set of common zeros in \mathbb{A}^n of polynomials $F_1, \dots, F_m \in \mathbb{K}[X_1, \dots, X_n]$. Correspondingly, a **projective \mathbb{K} -variety** is the set of common zeros in \mathbb{P}^n of a family of homogeneous polynomials $F_1, \dots, F_m \in \mathbb{K}[X_0, \dots, X_n]$. We shall frequently denote by $V(F_1, \dots, F_m)$ the affine or projective \mathbb{K} -variety consisting of the common zeros of polynomials F_1, \dots, F_m . The set $V(\mathbb{F}_q) := V \cap \mathbb{F}_q^n$ is the set of \mathbb{F}_q -rational points of V .

A \mathbb{K} -variety V is **\mathbb{K} -irreducible** if it cannot be expressed as a finite union of proper \mathbb{K} -subvarieties of V . Further, V is **absolutely irreducible** if it is $\overline{\mathbb{F}}_q$ -irreducible as a $\overline{\mathbb{F}}_q$ -variety. Any \mathbb{K} -variety V can be expressed as an irredundant union $V = \mathcal{C}_1 \cup \dots \cup \mathcal{C}_s$ of irreducible (absolutely irreducible) \mathbb{K} -varieties, unique up to reordering, which are called the **irreducible (absolutely irreducible) \mathbb{K} -components** of V .

For a \mathbb{K} -variety V contained in \mathbb{A}^n or \mathbb{P}^n , we denote by $I(V)$ its **defining ideal**, namely the set of polynomials of $\mathbb{K}[X_1, \dots, X_n]$, or of $\mathbb{K}[X_0, \dots, X_n]$, vanishing on V . The **coordinate ring** $\mathbb{K}[V]$ of V is defined as the quotient ring $\mathbb{K}[X_1, \dots, X_n]/I(V)$ or $\mathbb{K}[X_0, \dots, X_n]/I(V)$. The **dimension** $\dim V$ of a \mathbb{K} -variety V is the length r of the longest chain $V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_r$ of nonempty irreducible \mathbb{K} -varieties contained in V . A \mathbb{K} -variety V is called **equidimensional** if all the irreducible \mathbb{K} -components of V are of the same dimension.

The **degree** $\deg V$ of an irreducible \mathbb{K} -variety V is the maximum number of points lying in the intersection of V with a linear space L of codimension $\dim V$, for which $V \cap L$ is a finite set. More generally, following [Hei83] (see also [Ful84]), if $V = \mathcal{C}_1 \cup \dots \cup \mathcal{C}_s$ is the decomposition of V into irreducible \mathbb{K} -components, we define the degree of V as

$$\deg V := \sum_{i=1}^s \deg \mathcal{C}_i.$$

With this definition of degree, we have the following *Bézout inequality* (see [Hei83, Ful84, Vog84]): if V and W are \mathbb{K} -varieties, then

$$(3.2) \quad \deg(V \cap W) \leq \deg V \cdot \deg W.$$

Let V and W be irreducible affine \mathbb{K} -varieties of the same dimension and let $f : V \rightarrow W$ be a regular map for which $f(V) = W$ holds, where $f(V)$ denotes the closure of $f(V)$ with respect to the Zariski topology of W . Such a map is called **dominant**. Then f induces a ring extension $\mathbb{K}[W] \hookrightarrow \mathbb{K}[V]$ by composition with f . We say that the dominant map f is a **finite morphism** if this extension is integral, namely if each element $\eta \in \mathbb{K}[V]$ satisfies a monic equation with coefficients in $\mathbb{K}[W]$. A basic fact is that a dominant finite morphism is necessarily closed. Another fact concerning dominant finite morphisms we shall use in the sequel is that the preimage $f^{-1}(S)$ of an irreducible closed subset $S \subset W$ is equidimensional of dimension $\dim S$ (see, e.g., [Dan94, §4.2, Proposition]).

Let $V \subset \mathbb{A}^n$ be a variety and let $I(V) \subset \overline{\mathbb{F}}_q[X_1, \dots, X_n]$ be the defining ideal of V . Let \mathbf{x} be a point of V . The dimension $\dim_{\mathbf{x}} V$ of V at \mathbf{x} is the maximum of the dimensions of the irreducible components of V that contain \mathbf{x} . If $I(V) = (F_1, \dots, F_m)$, the tangent space $\mathcal{T}_{\mathbf{x}} V$ to V at \mathbf{x} is the kernel of the Jacobian matrix $(\partial F_i / \partial X_j)_{1 \leq i \leq m, 1 \leq j \leq n}(\mathbf{x})$ of F_1, \dots, F_m with respect to X_1, \dots, X_n at \mathbf{x} . The point \mathbf{x} is **regular** if $\dim \mathcal{T}_{\mathbf{x}} V = \dim_{\mathbf{x}} V$ holds. Otherwise, the point \mathbf{x} is called **singular**. The set of singular points of V is the **singular locus** $\text{Sing}(V)$ of V . A variety is called **nonsingular** if its singular locus is empty. For a projective variety, the concepts of tangent space, regular and singular point can be defined by considering an affine neighborhood of the point under consideration.

Elements F_1, \dots, F_r in $\overline{\mathbb{F}}_q[X_1, \dots, X_n]$ or in $\overline{\mathbb{F}}_q[X_0, \dots, X_n]$ form a **regular sequence** if F_1 is nonzero and each F_i is not a zero divisor in the quotient ring $\overline{\mathbb{F}}_q[X_1, \dots, X_n]/(F_1, \dots, F_{i-1})$ or $\overline{\mathbb{F}}_q[X_0, \dots, X_n]/(F_1, \dots, F_{i-1})$ for $2 \leq i \leq r$. In such a case, the (affine or projective) variety $V := V(F_1, \dots, F_r)$ they define is equidimensional of dimension $n - r$, and is called a **set-theoretic complete intersection**. If, in addition, the ideal (F_1, \dots, F_r) generated by F_1, \dots, F_r is radical, then V is an **ideal-theoretic complete intersection**. If $V \subset \mathbb{P}^n$ is an ideal-theoretic complete intersection of dimension $n - r$, and F_1, \dots, F_r is a system of homogeneous generators of $I(V)$, the degrees d_1, \dots, d_r depend only on V and not on the system of generators. Arranging the d_i in such a way that $d_1 \geq d_2 \geq \dots \geq d_r$, we call $\mathbf{d} := (d_1, \dots, d_r)$ the **multidegree** of V . The so-called *Bézout theorem* (see, e.g., [Har92, Theorem 18.3]) asserts that

$$(3.3) \quad \deg V = d_1 \cdots d_r.$$

In what follows we shall deal with a particular class of complete intersections, which we now define. A variety is **regular in codimension m** if the singular locus $\text{Sing}(V)$ of V has codimension at least $m + 1$ in V , namely if $\dim V - \dim \text{Sing}(V) \geq m + 1$. A complete intersection V which is regular in codimension 1 is called **normal** (actually, normality is a general notion that agrees on complete intersections with the one defined here). A fundamental result for projective complete intersections is the Hartshorne connectedness theorem (see, e.g., [Kun85, Theorem VI.4.2]), which we now state. If $V \subset \mathbb{P}^n$ is a set-theoretic complete intersection and $W \subset V$ is any subvariety of codimension at least 2, then $V \setminus W$ is connected in the Zariski topology of \mathbb{P}^n . Applying the Hartshorne connectedness theorem with $W := \text{Sing}(V)$, one deduces the following result.

Theorem 3.1. *If $V \subset \mathbb{P}^n$ is a normal set-theoretic complete intersection, then V is absolutely irreducible.*

3.2. The singular locus of the variety $V(R_1, \dots, R_m)$. With the notations and assumptions of the beginning of Section 3, let $V := V^{\lambda} \subset \mathbb{A}^n$ be the affine variety defined by the polynomials $R_1, \dots, R_m \in \mathbb{F}_q[\mathbf{X}]$ of (3.1). The main result of this section asserts that V is regular in codimension one. From this result we will be able to conclude that V is a normal ideal-theoretic complete intersection.

In the sequel we shall frequently express the points of \mathbb{A}^n in the coordinate system $\mathbf{Y} := (Y_1, \dots, Y_n)$, where Y_1, \dots, Y_n are the linear forms of (2.5). Let Z_1, \dots, Z_n be new indeterminates over $\overline{\mathbb{F}}_q$, set $\mathbf{Z} := (Z_1, \dots, Z_{n-r})$ and let $S_1, \dots, S_m \in \mathbb{F}_q[\mathbf{Z}]$ be the linear polynomials for which $R_j = S_j(\Pi_1, \dots, \Pi_{n-r})$ holds for $1 \leq j \leq m$, where Π_1, \dots, Π_{n-r} are the first $n - r$ elementary symmetric polynomials of $\overline{\mathbb{F}}_q[\mathbf{Y}]$.

Recall that, by hypothesis, the Jacobian matrix $(\partial \mathbf{S} / \partial \mathbf{Z})$ of $\mathbf{S} := (S_1, \dots, S_m)$ with respect to \mathbf{Z} has full rank m .

We now consider S_1, \dots, S_m as elements of $\mathbb{F}_q[Z_1, \dots, Z_n]$. Since the Jacobian matrix $(\partial \mathbf{S} / \partial \mathbf{Z})$ has full rank m , the linear affine variety $W \subset \mathbb{A}^n$ that S_1, \dots, S_m define has dimension $n - m$. Consider the following surjective mapping:

$$\begin{aligned} \mathbf{\Pi}^n : \mathbb{A}^n &\rightarrow \mathbb{A}^n \\ \mathbf{y} &\mapsto (\Pi_1(\mathbf{y}), \dots, \Pi_n(\mathbf{y})). \end{aligned}$$

It is easy to see that $\mathbf{\Pi}^n$ is a dominant finite morphism (see, e.g., [Sha94, §5.3, Example 1]). In particular, the preimage $(\mathbf{\Pi}^n)^{-1}(\mathcal{Z})$ of an irreducible affine variety $\mathcal{Z} \subset \mathbb{A}^n$ of dimension m is equidimensional and of dimension m .

Observe that the affine linear variety $W_j := V(S_1, \dots, S_j) \subset \mathbb{A}^n$ is equidimensional of dimension $n - j$. This implies that the affine variety $(\mathbf{\Pi}^n)^{-1}(W_j) = V(R_1, \dots, R_j) \subset \mathbb{A}^n$ is equidimensional of dimension $n - j$. We conclude that R_1, \dots, R_m form a regular sequence of $\mathbb{F}_q[\mathbf{Y}]$ and deduce the following result.

Lemma 3.2. *Let $V \subset \mathbb{A}^n$ be the affine variety defined by R_1, \dots, R_m . Then V is a set-theoretic complete intersection of dimension $n - m$.*

Next we analyze the dimension of the singular locus of V . Assume without loss of generality that $(\partial \mathbf{S} / \partial \mathbf{Z})$ is lower triangular in row-echelon form. Let $1 \leq i_1 < \dots < i_m \leq n - r$ be the indices corresponding to the pivots. Let $\mathcal{I} := \{i_1, \dots, i_m\}$ and $\mathcal{J} := \{j_1, \dots, j_{n-r-m}\} := \{1, \dots, n - r\} \setminus \mathcal{I}$. Then the Jacobian matrix

$$(3.4) \quad \mathcal{M} := (\partial(S_1, \dots, S_m, Z_{j_1}, \dots, Z_{j_{n-r-m}}) / \partial \mathbf{Z}) \in \overline{\mathbb{F}}_q^{(n-r) \times (n-r)}$$

is invertible. Let B_0, \dots, B_{n-m-1} be new indeterminates over $\overline{\mathbb{F}}_q$ and define $S_{m+k} := Z_{j_k} + B_{n-m-k}$ ($1 \leq k \leq n - r - m$) and $S_k := Z_k + B_{n-k}$ ($n - r + 1 \leq k \leq n$). Set $\mathbf{B} := (B_{n-m-1}, \dots, B_0)$, $\mathbf{S}^e := (S_1, \dots, S_n)$ and $\mathbf{Z}^e := (Z_1, \dots, Z_n)$. Observe that the Jacobian matrix

$$(\partial \mathbf{S}^e / \partial \mathbf{Z}^e) = (\partial(S_1, \dots, S_m, Z_{j_1}, \dots, Z_{j_{n-r-m}}, Z_{n-r+1}, \dots, Z_n) / \partial \mathbf{Z}^e)$$

is also invertible. Consider the following surjective morphism of affine varieties:

$$\begin{aligned} \mathbf{\Pi} : \mathbb{A}^n &\rightarrow \mathbb{A}^{n-r} \\ \mathbf{y} &\mapsto (\Pi_1(\mathbf{y}), \dots, \Pi_{n-r}(\mathbf{y})). \end{aligned}$$

Finally, we introduce the affine variety $V^e \subset \mathbb{A}^{2n-m}$ defined in the following way:

$$V^e := \{(\mathbf{y}, \mathbf{b}) \in \mathbb{A}^n \times \mathbb{A}^{n-m} : S_j(\mathbf{\Pi}(\mathbf{y}), \mathbf{b}) = 0 \ (1 \leq j \leq n)\}.$$

In order to establish a relation between V and V^e , let (\mathbf{y}, \mathbf{b}) be an arbitrary point of V^e . Then $S_j(\mathbf{\Pi}(\mathbf{y}), \mathbf{b}) = S_j(\mathbf{\Pi}(\mathbf{y})) = 0$ holds for $1 \leq j \leq m$, which implies that $\mathbf{y} \in V$. This shows the following regular mapping of affine varieties is well-defined:

$$\begin{aligned} \Phi_1^e : V^e &\rightarrow V \\ (\mathbf{y}, \mathbf{b}) &\mapsto \mathbf{y}. \end{aligned}$$

Furthermore, by the definition of V^e it is easy to see that Φ_1^e is an isomorphism of affine varieties, whose inverse is the following mapping:

$$\begin{aligned} \Psi^e : V &\rightarrow V^e \\ \mathbf{y} &\mapsto (\mathbf{y}, -\Pi_{j_1}(\mathbf{y}), \dots, -\Pi_{j_{n-r-m}}(\mathbf{y}), -\Pi_{n-r+1}(\mathbf{y}), \dots, -\Pi_n(\mathbf{y})). \end{aligned}$$

We conclude that V^e is an affine equidimensional variety of dimension $n - m$.

Our aim is to show that the singular locus Σ of V has codimension at least 2 in V . For this purpose, we shall show that the singular Σ^e of V^e has codimension at least 2 in V^e .

Let $R_{m+k} := S_{m+k}(\mathbf{\Pi}, \mathbf{B})$ for $1 \leq k \leq n-m$. We denote by $(\partial \mathbf{R}/\partial \mathbf{Y})$ the Jacobian matrix of $\mathbf{R} := (R_1, \dots, R_m)$ with respect to \mathbf{Y} and by $(\partial \mathbf{R}^e/\partial(\mathbf{Y}, \mathbf{B}))$ the Jacobian matrix of $\mathbf{R}^e := (R_1, \dots, R_n)$ with respect to \mathbf{Y} and \mathbf{B} . The relation between the singular locus of V and V^e is expressed in the following remark.

Remark 3.3. For $\mathbf{y} \in V$, let $(\mathbf{y}, \mathbf{b}) := \Psi^e(\mathbf{y})$. Then $(\partial \mathbf{R}/\partial \mathbf{Y})(\mathbf{y})$ is of full rank m if and only if $(\partial \mathbf{R}^e/\partial(\mathbf{Y}, \mathbf{B}))(\mathbf{y}, \mathbf{b})$ is of full rank n .

Proof. Let $\mathbf{y} \in V$ be a point as in the statement of the remark. By the definition of \mathbf{R}^e it follows that $(\partial \mathbf{R}^e/\partial(\mathbf{Y}, \mathbf{B}))(\mathbf{y}, \mathbf{b})$ has a block structure as follows:

$$\frac{\partial \mathbf{R}^e}{\partial(\mathbf{Y}, \mathbf{B})}(\mathbf{y}, \mathbf{b}) = \begin{pmatrix} \frac{\partial \mathbf{R}}{\partial \mathbf{Y}}(\mathbf{y}) & \mathbf{0} \\ \frac{\partial(\mathbf{R}^e \setminus \mathbf{R})}{\partial \mathbf{Y}}(\mathbf{y}, \mathbf{b}) & \frac{\partial(\mathbf{R}^e \setminus \mathbf{R})}{\partial \mathbf{B}}(\mathbf{y}, \mathbf{b}) \end{pmatrix} = \begin{pmatrix} \frac{\partial \mathbf{R}}{\partial \mathbf{Y}}(\mathbf{y}) & \mathbf{0} \\ \frac{\partial(\mathbf{R}^e \setminus \mathbf{R})}{\partial \mathbf{Y}}(\mathbf{y}, \mathbf{b}) & \mathbf{I} \end{pmatrix},$$

where $\mathbf{0}$ denotes a zero $m \times (n-m)$ -matrix and \mathbf{I} denotes an $(n-m) \times (n-m)$ -identity matrix. The conclusion of the remark readily follows. \square

In order to obtain an upper bound on the dimension of the singular locus of V^e , we consider the following projection mapping:

$$\begin{aligned} \Phi_2^e : V^e &\rightarrow \mathbb{A}^{n-m} \\ (\mathbf{y}, \mathbf{b}) &\mapsto \mathbf{b}. \end{aligned}$$

We shall analyze the image under Φ_2^e of the singular locus of V^e . The following result will allow us to draw conclusions concerning the singular locus of V^e from the analysis of its image under Φ_2^e .

Lemma 3.4. Φ_2^e is a dominant finite morphism.

Proof. Let $\alpha_i := S_i(\mathbf{0})$ for $1 \leq i \leq m$ and let $\boldsymbol{\alpha} := (\alpha_1, \dots, \alpha_m)$. Set $\mathbf{B}_J := (B_{n-m-1}, \dots, B_r)$. By the definition of the matrix \mathcal{M} of (3.4) it follows that

$$(R_1, \dots, R_{n-r}) = \mathcal{M} \cdot \mathbf{\Pi} + (\boldsymbol{\alpha}, \mathbf{B}_J)^t,$$

where $\mathbf{\Pi} := (\Pi_1, \dots, \Pi_{n-r})$. As a consequence, we have $\mathbf{\Pi}(\mathbf{y}) + \mathcal{M}^{-1}(\boldsymbol{\alpha}, \mathbf{b}_J)^t = \mathbf{0}$ for any $(\mathbf{y}, \mathbf{b}) \in V^e$. Denote by \mathbf{m}_j the j th row of \mathcal{M}^{-1} for $1 \leq j \leq n-r$. Then

$$\Pi_j(\mathbf{y}) + \mathbf{m}_j \cdot (\boldsymbol{\alpha}, \mathbf{b}_J)^t = 0 \quad (1 \leq j \leq n-r)$$

for any $(\mathbf{y}, \mathbf{b}) \in V^e$. Furthermore, the identity

$$(y_j)^n + \sum_{k=1}^n (-1)^k \Pi_k(\mathbf{y}) (y_j)^{n-k} = 0$$

holds for $1 \leq j \leq n$. Combining the two previous identities and the definition of \mathbf{S}^e , we conclude that the polynomial

$$P_j := Y_j^n - \sum_{k=1}^{n-r} (-1)^k \mathbf{m}_k \cdot (\boldsymbol{\alpha}, \mathbf{B}_J)^t Y_j^{n-k} - \sum_{k=n-r+1}^n (-1)^k B_{n-k} Y_j^{n-k}$$

vanishes identically over V^e for $1 \leq j \leq n$.

Let $\mathbf{b} \in \mathbb{A}^{n-m}$ be a point of the image of Φ_2^e and let $\mathbf{y} \in V$ be an arbitrary point with $(\mathbf{y}, \mathbf{b}) \in V^e$. As the identity $P_j(y_j, \mathbf{b}) = 0$ holds for $1 \leq j \leq n$, the fiber of \mathbf{b} under Φ_2^e has dimension zero. Then the theorem on the dimension of fibers (see, e.g.,

[Sha94, §I.6.3, Theorem 7]) asserts that $\dim V^e - \dim \Phi_2^e(V^e) \leq \dim(\Phi_2^e)^{-1}(\mathbf{b}) = 0$, namely $\dim \Phi_2^e(V^e) \geq n - m$. It follows that Φ_2^e is dominant.

Furthermore, since $P_j(Y_j, \mathbf{B}) = 0$ holds in $\overline{\mathbb{F}}_q[V^e]$ for $1 \leq j \leq n$, we see that the ring extension $\overline{\mathbb{F}}_q[\mathbf{B}] \hookrightarrow \overline{\mathbb{F}}_q[V^e]$ is integral. This implies that Φ_2^e is a finite morphism and finishes the proof of the lemma. \square

Next we obtain a partial characterization of the singular locus of V^e . Here we use the fact that V is defined by symmetric polynomials.

Lemma 3.5. *Let $(\mathbf{y}, \mathbf{b}) \in V^e$ be a point for which $(\partial \mathbf{R}^e / \partial (\mathbf{Y}, \mathbf{B}))(\mathbf{y}, \mathbf{b})$ has not full rank. Then there exist $1 \leq i < j < k < l \leq n$ such that $y_i = y_j$ and $y_k = y_l$.*

Proof. Let $(\mathbf{y}, \mathbf{b}) \in V^e$ be a point as in the statement of the lemma. According to Remark 3.3, the Jacobian matrix $(\partial \mathbf{R} / \partial \mathbf{Y})(\mathbf{y})$ is not of full rank. Since $\mathbf{R} = \mathbf{S} \circ \mathbf{\Pi}$, by the chain rule we obtain

$$\left(\frac{\partial \mathbf{R}}{\partial \mathbf{Y}} \right) = \left(\frac{\partial \mathbf{S}}{\partial \mathbf{Z}} \circ \mathbf{\Pi} \right) \cdot \left(\frac{\partial \mathbf{\Pi}}{\partial \mathbf{Y}} \right).$$

Let $\mathbf{v} \in \mathbb{A}^m$ a nonzero vector in the left kernel of $(\partial \mathbf{R} / \partial \mathbf{Y})(\mathbf{y})$. Then

$$\mathbf{0} = \mathbf{v} \cdot \left(\frac{\partial \mathbf{R}}{\partial \mathbf{Y}} \right) (\mathbf{y}) = \mathbf{v} \cdot \left(\frac{\partial \mathbf{S}}{\partial \mathbf{Z}} \right) (\mathbf{\Pi}(\mathbf{y})) \cdot \left(\frac{\partial \mathbf{\Pi}}{\partial \mathbf{Y}} \right) (\mathbf{y}).$$

Since the Jacobian matrix $(\partial \mathbf{S} / \partial \mathbf{Z})(\mathbf{\Pi}(\mathbf{y}))$ has full rank, we deduce that the vector $\mathbf{w} := \mathbf{v} \cdot (\partial \mathbf{S} / \partial \mathbf{Z})(\mathbf{\Pi}(\mathbf{y})) \in \mathbb{A}^{n-r}$ is nonzero and

$$\mathbf{w} \cdot \left(\frac{\partial \mathbf{\Pi}}{\partial \mathbf{Y}} \right) (\mathbf{y}) = \mathbf{0}.$$

Hence, all the maximal minors of $(\partial \mathbf{\Pi} / \partial \mathbf{Y})(\mathbf{y})$ must vanish.

Arguing as in the proof of [CMPP14, Theorem 3.2] (see also [CMP12b, Theorem 3.1]), we conclude that \mathbf{y} has at most $n - 4$ pairwise-distinct coordinates. In particular, there exist $1 \leq i < j \leq n - 2$ with $y_i = y_j$. Assume without loss of generality that $i = 1$ and $j = 2$. Then there exist $3 \leq k < l \leq n$ with $y_k = y_l$. This finishes the proof of the lemma. \square

Now we obtain an upper bound on the dimension of the singular locus of V^e .

Proposition 3.6. *Let $p > 2$. The set of points $(\mathbf{y}, \mathbf{b}) \in V^e$ for which the Jacobian matrix $(\partial \mathbf{R}^e / \partial (\mathbf{Y}, \mathbf{B}))(\mathbf{y}, \mathbf{b})$ has not full rank, has codimension at least 2 in V^e . In particular, the singular locus of V^e has codimension at least 2 in V^e .*

Proof. We use the notations of the proof of Lemma 3.4. In the proof of Lemma 3.4 we show that the polynomial

$$P_j(Y_j, \mathbf{B}) := Y_j^n - \sum_{k=1}^{n-r} (-1)^k \mathbf{m}_k \cdot (\boldsymbol{\alpha}, \mathbf{B}_J)^t Y_j^{n-k} - \sum_{k=n-r+1}^n (-1)^k B_{n-k} Y_j^{n-k}$$

vanishes identically on V^e for $1 \leq j \leq n$. Let $(\mathbf{y}, \mathbf{b}) \in V^e$ be a point as in the statement of the proposition and let $P_{\mathbf{b}} \in \overline{\mathbb{F}}_q[T]$ be the polynomial

$$\begin{aligned} P_{\mathbf{b}} &:= T^n - \sum_{k=1}^{n-r} (-1)^k \mathbf{m}_k \cdot (\boldsymbol{\alpha}, \mathbf{b}_J)^t T^{n-k} - \sum_{k=n-r+1}^n (-1)^k b_{n-k} T^{n-k} \\ &= T^n + \sum_{k=1}^n (-1)^k \Pi_k(\mathbf{y}) T^{n-k} = \prod_{j=1}^n (T - y_j). \end{aligned}$$

Since the roots of $P_{\mathbf{b}}$ in $\overline{\mathbb{F}}_q$ are the coordinates of \mathbf{y} , by Lemma 3.5 we have that $P_{\mathbf{b}}$ has either two distinct multiple roots, or a root of multiplicity at least three.

On one hand, [MPP13, Lemma 4.5] shows that the set consisting of the elements $\mathbf{b} \in \mathbb{A}^{n-m}$ such that $P_{\mathbf{b}}$ has two distinct multiple roots is contained in a subvariety of codimension 2 of \mathbb{A}^{n-m} . On the other hand, [MPP13, Lemma 4.7] proves that the subset of \mathbb{A}^{n-m} formed by the elements \mathbf{b} for which $P_{\mathbf{b}}$ has a root of multiplicity at least three is contained in a subvariety of codimension 2 of \mathbb{A}^{n-m} . As a consequence, the image under Φ_2^e of the set of points $(\mathbf{y}, \mathbf{b}) \in V^e$ as in the statement of the lemma is contained in a subvariety of codimension 2 of \mathbb{A}^{n-m} .

Lemma 3.4 asserts that Φ_2^e is dominant finite morphism. Therefore, as the inverse image of a codimension-2 subvariety of \mathbb{A}^{n-m} is a codimension-2 subvariety of V^e , the first assertion of the proposition is deduced.

Now we consider the second assertion of the proposition. Let (\mathbf{y}, \mathbf{b}) be a singular point of V^e and let $\mathcal{T}_{\mathbf{y}}V^e$ be the tangent space of V^e at \mathbf{y} . Since $V^e = V(R_1, \dots, R_n)$, for any $\mathbf{v} \in \mathcal{T}_{\mathbf{y}}V^e$ we have $(\partial \mathbf{R}^e / \partial \mathbf{Y})(\mathbf{y}, \mathbf{b}) \cdot \mathbf{v} = \mathbf{0}$. If the Jacobian matrix $(\partial \mathbf{R}^e / \partial \mathbf{Y})(\mathbf{y}, \mathbf{b})$ had full rank, then $\mathcal{T}_{\mathbf{y}}V^e$ would have dimension at most $n - m$, contradicting thus our assumption on (\mathbf{y}, \mathbf{b}) . Hence, the second assertion readily follows. \square

Finally, we are able to establish our main result concerning the dimension of the singular locus of V .

Theorem 3.7. *Let $p > 2$. The set of points $\mathbf{y} \in V$ for which $(\partial \mathbf{R} / \partial \mathbf{Y})(\mathbf{y})$ has not full rank, has codimension at least 2 in V . In particular, the singular locus Σ of V has codimension at least 2 in V .*

Proof. Recall that the projection mapping $\Phi_1^e : V^e \rightarrow V$ defined by $\Phi_1^e(\mathbf{y}, \mathbf{b}) := \mathbf{y}$ is an isomorphism of affine varieties. Furthermore, Remark 3.3 asserts that the image under Φ_1^e of the set of points $(\mathbf{y}, \mathbf{b}) \in V^e$ for which $(\partial \mathbf{R}^e / \partial (\mathbf{Y}, \mathbf{B}))(\mathbf{y}, \mathbf{b})$ has not full rank is the set of points $\mathbf{y} \in V$ as in the statement of the theorem. Proposition 3.6 shows that the former is contained in a codimension-2 subvariety of V^e , which implies that the latter is contained in a codimension-2 subvariety of V . This proves the first assertion of the theorem.

Now let \mathbf{y} be an arbitrary point Σ . By Lemma 3.2 we have $\dim \mathcal{T}_{\mathbf{y}}V > n - m$. This implies that $\text{rank}(\partial \mathbf{R} / \partial \mathbf{Y})(\mathbf{y}) < m$, for otherwise we would have $\dim \mathcal{T}_{\mathbf{y}}V \leq n - m$, contradicting thus the fact that \mathbf{y} is a singular point of V . From the first assertion, already proved, we easily deduce the second assertion of the theorem. \square

From Lemma 3.2 and Theorem 3.7 we obtain further algebraic and geometric consequences concerning the polynomials R_1, \dots, R_m and the variety V . By Theorem 3.7 we have that the set of points $\mathbf{y} \in V$ for which the Jacobian matrix $(\partial \mathbf{R} / \partial \mathbf{Y})(\mathbf{y})$ has not full rank has codimension at least 2 in V . Since R_1, \dots, R_m

form a regular sequence of $\mathbb{F}_q[\mathbf{Y}]$, from [Eis95, Theorem 18.15] we conclude that R_1, \dots, R_m define a radical ideal of $\mathbb{F}_q[\mathbf{Y}]$.

On the other hand, recall that the matrix $(\partial \mathbf{S} / \partial \mathbf{Z})$ was supposed to be lower triangular in row-echelon form, the indices i_1, \dots, i_m corresponding to the positions of the pivots of $(\partial \mathbf{S} / \partial \mathbf{Z})$. Then each polynomial R_j has degree i_j for $1 \leq j \leq m$. By the Bézout inequality (3.2) we have $\deg V \leq \prod_{j=1}^m \deg R_j = i_1 \cdots i_m$. In other words, we have the following statement.

Corollary 3.8. *Let $p > 2$. The polynomials R_1, \dots, R_m define a radical ideal and the variety V has degree $\deg V \leq \prod_{j=1}^m \deg R_j = i_1 \cdots i_m$.*

3.3. The projective closure of V . In order to obtain estimates on the number of \mathbb{F}_q -rational points of V we need information concerning the behavior of V “at infinity”. For this purpose, we consider the projective closure $\text{pcl}(V) \subset \mathbb{P}^n$ of V , whose definition we now recall. Consider the embedding of \mathbb{A}^n into the projective space \mathbb{P}^n which assigns to any $\mathbf{y} := (y_1, \dots, y_n) \in \mathbb{A}^n$ the point $(1 : y_1 : \cdots : y_n) \in \mathbb{P}^n$. The closure $\text{pcl}(V) \subset \mathbb{P}^n$ of the image of V under this embedding in the Zariski topology of \mathbb{P}^n is called the **projective closure** of V . The points of $\text{pcl}(V)$ lying in the hyperplane $\{Y_0 = 0\}$ are called the points of $\text{pcl}(V)$ at infinity.

It is well-known that $\text{pcl}(V)$ is the variety of \mathbb{P}^n defined by the homogenization $F^h \in \mathbb{F}_q[Y_0, \dots, Y_n]$ of each polynomial F belonging to the ideal $(R_1, \dots, R_m) \subset \mathbb{F}_q[Y_1, \dots, Y_n]$ (see, e.g., [Kun85, §I.5, Exercise 6]). Denote by $(R_1, \dots, R_m)^h$ the ideal generated by all the polynomials F^h with $F \in (R_1, \dots, R_m)$. Since the ideal (R_1, \dots, R_m) is radical, the ideal $(R_1, \dots, R_m)^h$ is also radical (see, e.g., [Kun85, §I.5, Exercise 6]). Furthermore, $\text{pcl}(V)$ is equidimensional of dimension $n - m$ (see, e.g., [Kun85, Propositions I.5.17 and II.4.1]) and degree equal to $\deg V$ (see, e.g., [CGH91, Proposition 1.11]).

Now we discuss the behavior of $\text{pcl}(V)$ at infinity. According to (3.1), each R_j can be expressed as

$$R_j = S_j(\Pi_1, \dots, \Pi_{n-r}) \quad (1 \leq j \leq m),$$

where $S_1, \dots, S_m \in \mathbb{F}_q[Z_1, \dots, Z_{n-r}]$ are elements of degree 1 whose Jacobian matrix $(\partial \mathbf{S} / \partial \mathbf{Z})$ with respect to $\mathbf{Z} := (Z_1, \dots, Z_{n-r})$ has full rank m . As before, we assume that $(\partial \mathbf{S} / \partial \mathbf{Z})$ is lower triangular in row-echelon form, namely there exist $1 \leq i_1 < i_2 < \cdots < i_m \leq n - r$ such that

$$R_j = \alpha_j + \sum_{k=1}^{i_j} c_{j,k} \Pi_k,$$

where $c_{j,i_j} \neq 0$ for $1 \leq j \leq m$. Hence, the homogenization of each R_j is the following polynomial of $\mathbb{F}_q[Y_0, \dots, Y_n]$:

$$(3.5) \quad R_j^h = \alpha_j Y_0^{i_j} + \sum_{k=1}^{i_j} c_{j,k} \Pi_k Y_0^{i_j-k}.$$

It follows that $R_j^h(0, Y_1, \dots, Y_n) = \Pi_{i_j}$ ($1 \leq j \leq m$). Observe that the polynomials $\Pi_{i_1}, \dots, \Pi_{i_m}$ are a possible choice for the polynomials R_1, \dots, R_m of (3.1). Therefore, Lemma 3.2, Theorem 3.7 and Corollary 3.8 hold with $R_j := \Pi_{i_j}$ for $1 \leq j \leq m$.

Lemma 3.9. *Let $p > 2$. Then $\text{pcl}(V)$ has singular locus at infinity of dimension at most $n - m - 3$.*

Proof. Let $\Sigma^\infty \subset \mathbb{P}^n$ denote the singular locus of $\text{pcl}(V)$ at infinity, namely the set of singular points of $\text{pcl}(V)$ lying in the hyperplane $\{Y_0 = 0\}$. Let $\mathbf{y} := (0 : y_1 : \dots : y_n)$ be an arbitrary point of Σ^∞ . Since the polynomials R_j^h vanish identically in $\text{pcl}(V)$, we have $R_j^h(\mathbf{y}) = \Pi_{i_j}(y_1, \dots, y_n) = 0$ for $1 \leq j \leq m$. Let $(\partial \Pi_{\mathcal{I}} / \partial \mathbf{Y})$ be the Jacobian matrix of $\Pi_{i_1}, \dots, \Pi_{i_m}$ with respect to Y_1, \dots, Y_n . We have

$$(3.6) \quad \text{rank} \left(\frac{\partial \Pi_{\mathcal{I}}}{\partial \mathbf{Y}} \right) (\mathbf{y}) < m,$$

for if not, we would have $\dim \mathcal{T}_{\mathbf{y}}(\text{pcl}(V)) \leq n - m$, which would imply that \mathbf{y} is a nonsingular point of $\text{pcl}(V)$, contradicting thus the hypothesis on \mathbf{y} .

Since the polynomials $\Pi_{i_1}, \dots, \Pi_{i_m}$ satisfy the hypotheses of Theorem 3.7, the points satisfying (3.6) form an affine equidimensional cone of dimension at most $n - m - 2$. We conclude that $\Sigma^\infty \subset \mathbb{P}^n$ has dimension at most $n - m - 3$. \square

Now we are able to completely characterize the behavior of $\text{pcl}(V)$ at infinity.

Theorem 3.10. *Let $p > 2$. Then $\text{pcl}(V) \cap \{Y_0 = 0\} \subset \mathbb{P}^{n-1}$ is a normal ideal-theoretic complete intersection of dimension $n - m - 1$ and degree $i_1 \cdots i_m$.*

Proof. From (3.5) it is easy to see that the polynomials $\Pi_{i_1}, \dots, \Pi_{i_m}$ vanish identically in $\text{pcl}(V) \cap \{Y_0 = 0\}$. Lemma 3.2, Theorem 3.7 and Corollary 3.8 show that the variety of \mathbb{A}^n defined by $\Pi_{i_1}, \dots, \Pi_{i_m}$ is an affine equidimensional cone of dimension $n - m$, degree at most $i_1 \cdots i_m$ and singular locus of dimension at most $n - m - 2$. It follows that the projective variety of \mathbb{P}^{n-1} defined by these polynomials is equidimensional of dimension $n - m - 1$, degree at most $i_1 \cdots i_m$ and singular locus of dimension at most $n - m - 3$.

Observe that $V(\Pi_{\mathcal{I}}) := V(\Pi_{i_1}, \dots, \Pi_{i_m}) \subset \mathbb{P}^{n-1}$ is a set-theoretic complete intersection, whose singular locus has codimension at least 2. We deduce that $V(\Pi_{\mathcal{I}})$ is normal and Theorem 3.1 shows that it is absolutely irreducible.

On the other hand, since $\text{pcl}(V)$ is equidimensional of dimension $n - m$, each irreducible component of $\text{pcl}(V) \cap \{Y_0 = 0\}$ has dimension at least $n - m - 1$. Furthermore, $\text{pcl}(V) \cap \{Y_0 = 0\}$ is contained in the projective variety $V(\Pi_{\mathcal{I}})$, which is absolutely irreducible of dimension $n - m - 1$. We conclude that $\text{pcl}(V) \cap \{Y_0 = 0\}$ is also absolutely irreducible of dimension $n - m - 1$, and hence

$$\text{pcl}(V) \cap \{Y_0 = 0\} = V(\Pi_{i_1}, \dots, \Pi_{i_m}).$$

Finally, by [Eis95, Theorem 18.15] we see that $\Pi_{i_1}, \dots, \Pi_{i_m}$ define a radical ideal. As a consequence of the Bézout theorem (3.3), $\deg(\text{pcl}(V) \cap \{Y_0 = 0\}) = \prod_{j=1}^m \deg \Pi_{i_j} = i_1 \cdots i_m$. This finishes the proof of the theorem. \square

We conclude this section with a statement that summarizes all the facts we shall need concerning the projective closure $\text{pcl}(V)$.

Theorem 3.11. *Let $p > 2$. Then $\text{pcl}(V) \subset \mathbb{P}^n$ is a normal ideal-theoretic complete intersection of dimension $n - m$ and degree $i_1 \cdots i_m$.*

Proof. We have already shown that $\text{pcl}(V)$ is equidimensional of dimension $n - m$ and degree at most $i_1 \cdots i_m$. According to Theorem 3.7, the singular locus of $\text{pcl}(V)$ lying in the open set $\{Y_0 \neq 0\}$ has dimension at most $n - m - 2$, while Lemma 3.9 shows that its singular locus at infinity has dimension at most $n - m - 3$. We conclude that the singular locus of $\text{pcl}(V)$ has dimension at most $n - m - 2$.

Observe that $\text{pcl}(V)$ is contained in the projective variety $V(\mathbf{R}^h) := V(R_j^h : 1 \leq j \leq m)$. We have the inclusions

$$V(\mathbf{R}^h) \cap \{Y_0 \neq 0\} \subset V(\mathbf{R}), \quad V(\mathbf{R}^h) \cap \{Y_0 = 0\} \subset V(\Pi_{\mathcal{I}}).$$

Both $\{R_j : 1 \leq j \leq m\}$ and $\{\Pi_{i_j} : 1 \leq j \leq m\}$ satisfy the conditions of the statement of Lemma 3.2. It follows that $V(\mathbf{R}) \subset \mathbb{A}^n$ is equidimensional of dimension $n - m$ and $V(\Pi_{\mathcal{I}}) \subset \mathbb{P}^{n-1}$ is equidimensional of dimension $n - m - 1$. We conclude that $V(\mathbf{R}^h) \subset \mathbb{P}^n$ has dimension at most $n - m$. Taking into account that it is defined by m polynomials, we deduce that it is a set-theoretic complete intersection of dimension $n - m$. This implies that it is equidimensional of dimension $n - m$, and therefore has no irreducible component contained in the hyperplane at infinity. In particular, it agrees with the projective closure of its restriction to \mathbb{A}^n (see, e.g., [Kun85, Proposition I.5.17]). As such a restriction is the affine variety $V = V(\mathbf{R})$, we deduce that

$$\text{pcl}(V) = V(\mathbf{R}^h).$$

Since its singular locus has codimension at least 2, we have that $V(\mathbf{R}^h)$ is a normal set-theoretic complete intersection. Finally, by [Eis95, Theorem 18.15] we see that the polynomials R_j^h ($1 \leq j \leq m$) define a radical ideal. Then the Bézout theorem (3.3) implies $\deg \text{pcl}(V) = \prod_{j=1}^m \deg R_j^h = i_1 \cdots i_m$ and finishes the proof of the theorem. \square

4. THE NUMBER OF POLYNOMIALS IN \mathcal{A}_{λ}

Let A_r, \dots, A_{n-1} be indeterminates over $\overline{\mathbb{F}}_q$ and set $\mathbf{A} := (A_{n-1}, \dots, A_r)$. Let be given linear forms $L_1, \dots, L_m \in \mathbb{F}_q[\mathbf{A}]$ which are linearly independent and $\alpha := (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m$. Set $\mathbf{L} := (L_1, \dots, L_m)$ and let $\mathcal{A} := \mathcal{A}(\mathbf{L}, \alpha)$ be the set defined in the following way:

$$\mathcal{A} := \{T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathbb{F}_q[T] : L_j(a_r, \dots, a_{n-1}) + \alpha_j = 0 \ (1 \leq j \leq m)\}.$$

As before, we shall assume that the Jacobian matrix $(\partial \mathbf{L} / \partial \mathbf{A})$ is lower triangular in row echelon form and denote by $1 \leq i_1 < \cdots < i_m \leq n - r$ the positions corresponding to the pivots. Given a factorization pattern $\lambda := 1^{\lambda_1} \cdots n^{\lambda_n}$, in this section we determine the asymptotic behavior of the cardinality of the set \mathcal{A}_{λ} of elements of \mathcal{A} with factorization pattern λ .

For this purpose, in Corollary 2.4 we obtain polynomials $R_1, \dots, R_m \in \mathbb{F}_q[\mathbf{X}] := \mathbb{F}_q[X_1, \dots, X_n]$ whose common \mathbb{F}_q -rational zeros are related to the quantity $|\mathcal{A}_{\lambda}|$. More precisely, let $\mathbf{x} := (\mathbf{x}_{i,j} : 1 \leq i \leq n, 1 \leq j \leq \lambda_i) \in \mathbb{F}_q^n$ be a common \mathbb{F}_q -rational zero of R_1, \dots, R_m of type λ (see Definition 2.1). We associate to \mathbf{x} an element $f \in \mathcal{A}_{\lambda}$ having $Y_{\ell_{i,j}+k}(\mathbf{x}_{i,j})$ as an \mathbb{F}_q -root for $1 \leq i \leq n$, $1 \leq j \leq \lambda_i$ and $1 \leq k \leq i$. Here, $Y_{\ell_{i,j}+k}$ is the linear form

$$(4.1) \quad Y_{\ell_{i,j}+k} := X_{\ell_{i,j}+1}\sigma_{k,i}(\theta_i) + \cdots + X_{\ell_{i,j}+i}\sigma_{k,i}(\theta_i^{q^{i-1}}),$$

where $\{\sigma_{k,i} : 1 \leq k \leq i\}$ are the elements of the Galois group \mathbb{G}_i of \mathbb{F}_{q^i} over \mathbb{F}_q .

Let $\mathcal{A}_{\lambda}^{sq} := \{f \in \mathcal{A}_{\lambda} : f \text{ is square-free}\}$ and let $\mathcal{A}_{\lambda}^{nsq} := \mathcal{A}_{\lambda} \setminus \mathcal{A}_{\lambda}^{sq}$. Corollary 2.4 asserts that any element $f \in \mathcal{A}_{\lambda}^{sq}$ is associated with $w(\lambda) := \prod_{i=1}^n i^{\lambda_i} \lambda_i!$ common \mathbb{F}_q -rational zeros of R_1, \dots, R_m of type λ . Observe that $\mathbf{x} \in \mathbb{F}_q^n$ is of type λ if and only if $Y_{\ell_{i,j}+k_1}(\mathbf{x}) \neq Y_{\ell_{i,j}+k_2}(\mathbf{x})$ for $1 \leq i \leq n$, $1 \leq j \leq \lambda_i$ and $1 \leq k_1 < k_2 \leq i$. Furthermore, $\mathbf{x} \in \mathbb{F}_q^n$ of type λ is associated with $f \in \mathcal{A}_{\lambda}^{sq}$ if and only if

$Y_{\ell_{i,j_1}+k_1}(\mathbf{x}) \neq Y_{\ell_{i,j_2}+k_2}(\mathbf{x})$ for $1 \leq i \leq n$, $1 \leq j_1 < j_2 \leq \lambda_i$ and $1 \leq k_1 < k_2 \leq i$. As a consequence, we see that

$$(4.2) \quad |\mathcal{A}_{\lambda}^{sq}| = \mathcal{T}(\lambda) \left| \left\{ \mathbf{x} \in \mathbb{F}_q^n : R_1(\mathbf{x}) = \cdots = R_m(\mathbf{x}) = 0, Y_{\ell_{i,j_1}+k_1}(\mathbf{x}) \neq Y_{\ell_{i,j_2}+k_2}(\mathbf{x}) \right. \right. \\ \left. \left. (1 \leq i \leq n, 1 \leq j_1 < j_2 \leq \lambda_i, 1 \leq k_1 < k_2 \leq i) \right\} \right|,$$

where $\mathcal{T}(\lambda) := 1/w(\lambda)$. The results of Section 3 will allow us to establish the asymptotic behavior of $|\mathcal{A}_{\lambda}^{sq}|$.

4.1. The number of \mathbb{F}_q -rational points of normal complete intersections.

Let $V \subset \mathbb{A}^n$ be the variety defined by the polynomials $R_1, \dots, R_m \in \mathbb{F}_q[\mathbf{X}]$ of (3.1). Denote by $\text{pcl}(V) \subset \mathbb{P}^n$ the projective closure of V and by $\text{pcl}(V)^\infty := \text{pcl}(V) \cap \{Y_0 = 0\} \subset \mathbb{P}^{n-1}$ the set of points of $\text{pcl}(V)$ at infinity. Theorems 3.10 and 3.11 assert that $\text{pcl}(V)^\infty$ and $\text{pcl}(V)$ are \mathbb{F}_q -definable normal ideal-theoretic complete intersections of dimension $n-m-1$ and $n-m$ respectively, both of degree $\delta_{\mathbf{L}} := i_1 \cdots i_m$.

In what follows, we shall use an estimate on the number of \mathbb{F}_q -rational points of a projective normal complete intersection of [CMP12a] (see also [CM07] or [GL02] for other estimates). More precisely, if $W \subset \mathbb{P}^n$ is a normal complete intersection defined over \mathbb{F}_q of dimension $n-l \geq 2$, degree δ and multidegree $\mathbf{d} := (d_1, \dots, d_l)$, then the following estimate holds (see [CMP12a, Theorem 1.3]):

$$(4.3) \quad \left| |W(\mathbb{F}_q)| - p_{n-l} \right| \leq (\delta(D-2) + 2)q^{n-l-\frac{1}{2}} + 14D^2\delta^2q^{n-l-1},$$

where $p_{n-l} := q^{n-l} + q^{n-l-1} + \cdots + q + 1 = |\mathbb{P}^{n-l}(\mathbb{F}_q)|$ and $D := \sum_{i=1}^l (d_i - 1)$.

First we estimate the number of \mathbb{F}_q -rational points of V . By (4.3), we have

$$\begin{aligned} \left| |\text{pcl}(V)(\mathbb{F}_q)| - p_{n-m} \right| &\leq (\delta_{\mathbf{L}}(D_{\mathbf{L}} - 2) + 2)q^{n-m-\frac{1}{2}} + 14D_{\mathbf{L}}^2\delta_{\mathbf{L}}^2q^{n-m-1}, \\ \left| |\text{pcl}(V)^\infty(\mathbb{F}_q)| - p_{n-m-1} \right| &\leq (\delta_{\mathbf{L}}(D_{\mathbf{L}} - 2) + 2)q^{n-m-\frac{3}{2}} + 14D_{\mathbf{L}}^2\delta_{\mathbf{L}}^2q^{n-m-2}, \end{aligned}$$

where $\delta_{\mathbf{L}} := i_1 \cdots i_m$ and $D_{\mathbf{L}} := \sum_{j=1}^m (i_j - 1)$. Hence, we obtain

$$(4.4) \quad \begin{aligned} \left| |V(\mathbb{F}_q)| - q^{n-m} \right| &= \left| |\text{pcl}(V)(\mathbb{F}_q)| - |\text{pcl}(V)^\infty(\mathbb{F}_q)| - p_{n-m} + p_{n-m-1} \right| \\ &\leq \left| |\text{pcl}(V)(\mathbb{F}_q)| - p_{n-m} \right| + \left| |\text{pcl}(V)^\infty(\mathbb{F}_q)| - p_{n-m-1} \right| \\ &\leq (q+1)q^{n-m-2}((\delta_{\mathbf{L}}(D_{\mathbf{L}} - 2) + 2)q^{1/2} + 14D_{\mathbf{L}}^2\delta_{\mathbf{L}}^2). \end{aligned}$$

Let $V^=$ be the affine subvariety of $V \subset \mathbb{A}^n$ defined by

$$V^= := \bigcup_{\substack{1 \leq i \leq n \\ 1 \leq j_1 < j_2 \leq \lambda_i, 1 \leq k_1 < k_2 \leq i}} V \cap \{Y_{\ell_{i,j_1}+k_1} = Y_{\ell_{i,j_2}+k_2}\},$$

where $Y_{\ell_{i,j}+k}$ are the linear forms of (4.1). Then (4.2) shows that $V^=$ represents the vector of coefficients of roots of non square-free polynomials. Let $V^\neq(\mathbb{F}_q) := V(\mathbb{F}_q) \setminus V^=(\mathbb{F}_q)$. Observe that (4.2) we may reexpressed as

$$(4.5) \quad |\mathcal{A}_{\lambda}^{sq}| = \mathcal{T}(\lambda) |V^\neq(\mathbb{F}_q)|$$

By the equality $\mathcal{T}(\lambda)|V^\neq(\mathbb{F}_q)| = \mathcal{T}(\lambda)|V(\mathbb{F}_q)| - \mathcal{T}(\lambda)|V^=(\mathbb{F}_q)|$ and (4.5), we obtain

$$\begin{aligned}
(4.6) \quad ||\mathcal{A}_\lambda| - \mathcal{T}(\lambda)q^{n-m}| &= ||\mathcal{A}_\lambda^{sq}| + |\mathcal{A}_\lambda^{nsq}| - \mathcal{T}(\lambda)q^{n-m}| \\
&= |\mathcal{T}(\lambda)|V^\neq(\mathbb{F}_q)| + |\mathcal{A}_\lambda^{nsq}| - \mathcal{T}(\lambda)q^{n-m}| \\
&= |\mathcal{T}(\lambda)|V(\mathbb{F}_q)| - \mathcal{T}(\lambda)|V^=(\mathbb{F}_q)| + |\mathcal{A}_\lambda^{nsq}| - \mathcal{T}(\lambda)q^{n-m}| \\
&\leq \mathcal{T}(\lambda)||V(\mathbb{F}_q)| - q^{n-m}| + ||\mathcal{A}_\lambda^{nsq}| - \mathcal{T}(\lambda)|V^=(\mathbb{F}_q)||.
\end{aligned}$$

The first term in the right-hand side is bounded using (4.4). On the other hand,

$$(4.7) \quad ||\mathcal{A}_\lambda^{nsq}| - \mathcal{T}(\lambda)|V^=(\mathbb{F}_q)|| = |\mathcal{A}_\lambda^{nsq}| - \mathcal{T}(\lambda)|V^=(\mathbb{F}_q)| \leq |\mathcal{A}_\lambda^{nsq}|.$$

As a consequence, by (4.4), (4.6) and (4.7) we obtain the following result.

Theorem 4.1. *For $p > 2$, $q > n$ and $3 \leq r \leq n - m$, we have*

$$\begin{aligned}
||\mathcal{A}_\lambda| - \mathcal{T}(\lambda)q^{n-m}| &\leq \\
&\leq (q+1)q^{n-m-2}\mathcal{T}(\lambda)\left((\delta_{\mathbf{L}}(D_{\mathbf{L}}-2)+2)q^{\frac{1}{2}}+14D_{\mathbf{L}}^2\delta_{\mathbf{L}}^2\right)+|\mathcal{A}_\lambda^{nsq}|,
\end{aligned}$$

where $\delta_{\mathbf{L}} := i_1 \cdots i_m$ and $D_{\mathbf{L}} := \sum_{j=1}^m (i_j - 1)$.

It remains to obtain an upper bound on the number $|\mathcal{A}_\lambda^{nsq}|$ of polynomials in \mathcal{A}_λ which are not square-free. To this end, observe that a polynomial $f \in \mathcal{A}$ is not square-free if and only if its discriminant is equal to zero. In [MPP13] we study the so-called *discriminant locus* of \mathcal{A} , namely the set \mathcal{A}^{nsq} formed by the elements of \mathcal{A} whose discriminant is equal to zero (see also [FS84] for further results on discriminant loci). According to [MPP13, Theorem A.3], the discriminant locus \mathcal{A}^{nsq} is the set of \mathbb{F}_q -rational points of a hypersurface of degree $n(n-1)$ of a suitable $(n-m)$ -dimensional affine space. As a consequence, by, e.g., [CM06, Lemma 2.1], we have

$$(4.8) \quad |\mathcal{A}_\lambda^{nsq}| \leq |\mathcal{A}^{nsq}| \leq n(n-1)q^{n-m-1}.$$

Combining Theorem 4.1 (with a slightly simplified bound) and (4.8) we deduce the following result.

Theorem 4.2. *For $p > 2$, $q > n$ and $3 \leq r \leq n - m$, we have*

$$(4.9) \quad ||\mathcal{A}_\lambda| - \mathcal{T}(\lambda)q^{n-m}| \leq q^{n-m-1}(2\mathcal{T}(\lambda)D_{\mathbf{L}}\delta_{\mathbf{L}}q^{\frac{1}{2}}+19\mathcal{T}(\lambda)D_{\mathbf{L}}^2\delta_{\mathbf{L}}^2+n(n-1)).$$

4.2. Factorization patterns of polynomials with prescribed coefficients.

In this section we briefly indicate how Theorem 4.2 is applied when \mathcal{A} consists of the polynomials of \mathcal{P} with certain prescribed coefficients. Given $0 < i_1 < i_2 < \cdots < i_m \leq n$ and $\alpha := (\alpha_{i_1}, \dots, \alpha_{i_m}) \in \mathbb{F}_q^m$, set $\mathcal{I} := \{i_1, \dots, i_m\}$ and

$$(4.10) \quad \mathcal{A}^m := \mathcal{A}^m(\mathcal{I}, \alpha) := \{T^n + a_1T^{n-1} + \cdots + a_n \in \mathbb{F}_q[T] : a_{i_j} = \alpha_{i_j} \ (1 \leq j \leq m)\}.$$

For a given factorization pattern λ , let $G \in \mathbb{F}_q[\mathbf{X}, T]$ be the polynomial of (2.4). According to Lemma 2.3, an element $f \in \mathcal{A}^m$ has factorization pattern λ if and only if there exists \mathbf{x} of type λ such that

$$(4.11) \quad (-1)^{i_j} \Pi_{i_j}(\mathbf{Y}(\mathbf{x})) = \alpha_{i_j} \quad (1 \leq j \leq m).$$

Therefore, applying Theorem 4.2 with $\delta_{\mathcal{I}} := i_1 \cdots i_m$ and $D_{\mathcal{I}} := \sum_{j=1}^m (i_j - 1)$, we obtain the following result.

Corollary 4.3. *For $p > 2$, $q > n$ and $i_m \leq n - 3$, we have*

$$||\mathcal{A}_\lambda^m| - \mathcal{T}(\lambda) q^{n-m}| \leq q^{n-m-1} (2 \mathcal{T}(\lambda) D_{\mathcal{I}} \delta_{\mathcal{I}} q^{\frac{1}{2}} + 19 \mathcal{T}(\lambda) D_{\mathcal{I}}^2 \delta_{\mathcal{I}}^2 + n(n-1)).$$

5. THE NUMBER OF POLYNOMIALS IN \mathcal{A}_λ IN THE SPARSE CASE

In [CMP12b], [CMPP14] and [MPP13] a methodology to deal with combinatorial problems over finite fields is developed. It is based on the fact that many combinatorial problems can be described by means of symmetric polynomials, and varieties defined by symmetric polynomials have particular features that can be exploited in order to obtain “good” estimates on their number of \mathbb{F}_q -rational points. A new avatar of these assertions can be seen in Sections 3 and 4 above.

In particular, similar techniques as in [CMPP14] can be applied in order to obtain a further estimate on the number of elements in \mathcal{A}_λ , which holds when the linear forms L_1, \dots, L_m are “sparse”. More precisely, if L_1, \dots, L_m are linearly independent elements of $\mathbb{F}_q[A_r, \dots, A_{n-1}]$ with $r \geq m+2$, then we will be able to show that

$$||\mathcal{A}_\lambda| - \mathcal{T}(\lambda) q^{n-m}| = \mathcal{O}(q^{n-m-1}),$$

improving thus the $\mathcal{O}(q^{n-m-\frac{1}{2}})$ estimate of the left-hand side of Theorem 4.2. We remark that this estimate is valid without restrictions on the characteristic of \mathbb{F}_q .

As the arguments differ slightly from the ones of [CMPP14] we shall merely sketch the approach. Roughly speaking, the results of [CMPP14] allows us to deduce that the singular locus of the variety V defined by the polynomials of (3.1) has codimension at least 3. Combining this with results about the geometry of V of Section 3 we conclude that its projective closure $\text{pcl}(V)$ is regular in codimension 2. Our estimate then follows from estimates on the number of \mathbb{F}_q -rational points of complete intersections which are regular in codimension 2 due to [CMP12a].

5.1. The geometry of the set of zeros of R_1, \dots, R_m for large r . Let be given r with $m+2 \leq r \leq n-m$, let A_r, \dots, A_{n-1} be indeterminates over $\overline{\mathbb{F}}_q$ and let L_1, \dots, L_m be linear forms of $\mathbb{F}_q[A_r, \dots, A_{n-1}]$ which are linearly independent. For $\alpha := (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m$, we set $\mathbf{L} := (L_1, \dots, L_m)$ and consider as before the linear variety $\mathcal{A} := \mathcal{A}(\mathbf{L}, \alpha)$ defined as

$$\mathcal{A} := \{T^n + a_{n-1}T^{n-1} + \dots + a_0 \in \mathbb{F}_q[T] : \mathbf{L}(a_r, \dots, a_{n-1}) + \alpha = \mathbf{0}\}.$$

Let R_1, \dots, R_m be the polynomials of $\mathbb{F}_q[\mathbf{X}] := \mathbb{F}_q[X_1, \dots, X_n]$ defined as

$$(5.1) \quad R_j := S_j(\Pi_1, \dots, \Pi_{n-r}) \quad (1 \leq j \leq m)$$

where Π_1, \dots, Π_{n-r} are the first $n-r$ elementary symmetric polynomials of $\mathbb{F}_q[Y_1, \dots, Y_n]$, $\mathbf{Y} := (Y_1, \dots, Y_n)$ is the vector of linear forms of $\overline{\mathbb{F}}_q[\mathbf{X}]$ defined as in (2.5) and the linear polynomials $S_1, \dots, S_m \in \mathbb{F}_q[Z_1, \dots, Z_{n-r}]$ are defined as in (3.1). According to Corollary 2.4, we can express the number of elements of \mathcal{A}_λ in terms of the number of \mathbb{F}_q -rational points of the variety $V \subset \mathbb{A}^n$ defined by R_1, \dots, R_m .

As in the previous sections, we assume that the Jacobian matrix $(\partial \mathbf{L} / \partial \mathbf{A})$ of the vector of linear forms \mathbf{L} with respect to $\mathbf{A} := (A_{n-1}, \dots, A_r)$ is lower triangular in row-echelon form. Hence, there exist $1 \leq i_1 < i_2 < \dots < i_m \leq n-r$ such that

$\deg R_j = i_j$ ($1 \leq j \leq m$). As before, the numbers

$$(5.2) \quad \delta_{\mathbf{L}} := i_1 \cdots i_m \quad \text{and} \quad D_{\mathbf{L}} := \sum_{j=1}^m (i_j - 1)$$

will play a central role in our estimates.

Next we show that the projective closure $\text{pcl}(V)$ of V and the set $\text{pcl}(V)^\infty$ of points of $\text{pcl}(V)$ at infinity are complete intersections which are regular in codimension two. For this purpose, we rely on results on the geometry of complete intersections defined by symmetric polynomials of [CMPP14, Section 3].

Theorem 5.1. *Let be given positive integers m , r and n with $q > n$ and $m + 2 \leq r \leq n - m$. Let R_1, \dots, R_m be the polynomials of (5.1) and $V \subset \mathbb{A}^n$ the affine variety defined by R_1, \dots, R_m . Then*

- (1) *V is an ideal-theoretic complete intersection of dimension $n - m$ and $\deg(V) \leq \prod_{i=1}^m \deg(R_i)$.*
- (2) *The set of points $\mathbf{y} \in \mathbb{A}^n$ for which $(\partial \mathbf{R} / \partial \mathbf{Y})(\mathbf{y})$ has not full rank, has dimension at most $n - r - 1$. In particular, the singular locus of V has dimension at most $n - r - 1$.*

Proof. As $S_1, \dots, S_m \in \mathbb{F}_q[Z_1, \dots, Z_{n-r}]$ are linear polynomials which are linearly independent, the hypotheses (H1) and (H2) of [CMPP14, Section 3.2] are satisfied. Then [CMPP14, Theorem 3.2] shows the second assertion. Finally, from [CMPP14, Corollary 3.3] we readily deduce the first assertion of the theorem. \square

If the polynomials R_1, \dots, R_m of (5.1) are homogeneous (for example, if $R_j = \Pi_{i_j}$ for $1 \leq j \leq m$), we may somewhat strengthen the conclusions of Theorem 5.1, as the next result asserts.

Corollary 5.2. *Let notations and assumptions be as above. Suppose further that R_1, \dots, R_m are homogeneous. Then*

- (1) *The projective variety $\mathcal{V} \subset \mathbb{P}^{n-1}$ defined by R_1, \dots, R_m is an ideal-theoretic complete intersection of dimension $n - m - 1$ and $\deg(\mathcal{V}) = \prod_{i=1}^m \deg(R_i)$.*
- (2) *The set of points $\mathbf{y} \in \mathbb{P}^{n-1}$ for which $(\partial \mathbf{R} / \partial \mathbf{Y})(\mathbf{y})$ has not full rank, has dimension at most $n - r - 2$. In particular, the singular locus of \mathcal{V} has dimension at most $n - r - 2$.*

Proof. The second assertion readily follows from that of Theorem 5.1. On the other hand, the first assertion of Theorem 5.1 implies that R_1, \dots, R_m form a regular sequence and define a radical ideal. Therefore, \mathcal{V} is an ideal-theoretic complete intersection of dimension $n - m - 1$. As a consequence, the Bézout theorem (3.3) shows that $\deg(\mathcal{V}) = \prod_{i=1}^m \deg(R_i)$. \square

As before, we consider the projective closure $\text{pcl}(V) \subset \mathbb{P}^n$ of the affine variety $V \subset \mathbb{A}^n$ defined by the polynomials R_1, \dots, R_m of (5.1) with respect to the embedding of \mathbb{A}^n into \mathbb{P}^n defined as $(y_1, \dots, y_n) \mapsto (1 : y_1 : \dots : y_n)$. We also denote by $\text{pcl}(V)^\infty$ the set of points of $\text{pcl}(V)$ at infinity, namely $\text{pcl}(V)^\infty := \text{pcl}(V) \cap \{Y_0 = 0\}$. In connection with the latter, we observe that, if R_j^h is the homogenization of R_j defined as in (3.5), the polynomials $R_j^h(0, Y_1, \dots, Y_n) = \Pi_{i_j}$ ($1 \leq j \leq m$) satisfy the hypotheses of Corollary 5.2. The next theorem summarizes all the properties of $\text{pcl}(V)$ and $\text{pcl}(V)^\infty$ which are relevant for our purposes.

Theorem 5.3. *Let n, m and r be positive integers with $q > n$ and $m + 2 \leq r \leq n - m$. The projective varieties $\text{pcl}(V) \subset \mathbb{P}^n$ and $\text{pcl}(V)^\infty := \text{pcl}(V) \cap \{Y_0 = 0\} \subset \mathbb{P}^{n-1}$ are ideal-theoretic complete intersections defined over \mathbb{F}_q , of dimension $n - m$ and $n - m - 1$ respectively, both of degree $\delta_{\mathbf{L}}$, having singular locus of dimension at most $n - r - 1$ and $n - r - 2$ respectively.*

Sketch of the proof. The proof of the assertions concerning $\text{pcl}(V)$ follows the lines of that of Theorem 3.11, applying Theorem 5.1 and Corollary 5.2 instead of Theorem 3.7 and Lemma 3.9. On the other hand, the assertions about $\text{pcl}(V)^\infty$ are shown following the proof of Theorem 3.10, using Corollary 5.2 instead of Lemma 3.2, Theorem 3.7 and Lemma 3.9. \square

5.2. The estimate of $|\mathcal{A}_{\lambda}|$ for large r . In what follows, we shall use an estimate on the number of \mathbb{F}_q -rational points of a projective singular complete intersection defined over \mathbb{F}_q due to [CMP12a] (see [GL02] for similar estimates). More precisely, if $W \subset \mathbb{P}^n$ is an \mathbb{F}_q -definable ideal-theoretic complete intersection of dimension $n - l$, degree $\delta \geq 2$, multidegree (d_1, \dots, d_l) and singular locus of dimension at most $n - l - 3$, then the following estimate holds (see [CMP12a, Corollary 8.4]):

$$(5.3) \quad |W(\mathbb{F}_q)| - p_{n-l} \leq 14D^3\delta^2q^{n-l-1},$$

where $D := \sum_{i=1}^l (d_i - 1)$.

As before, let be given positive integers m, n and r with $q > n$ and $m + 2 \leq r \leq n - m$. Let $V \subset \mathbb{A}^n$ be the variety defined by the polynomials R_1, \dots, R_m of (5.1) and let $\delta_{\mathbf{L}}$ and $D_{\mathbf{L}}$ be defined as in (5.2). Theorem 5.3 shows that the projective closure $\text{pcl}(V)$ of V and its set of points at infinity $\text{pcl}(V)^\infty$ satisfy all the requirements of [CMP12a, Corollary 8.4]. Then (5.3) implies

$$\begin{aligned} |\text{pcl}(V)(\mathbb{F}_q)| - p_{n-m} &\leq 14D_{\mathbf{L}}^3\delta_{\mathbf{L}}^2q^{n-m-1}, \\ |\text{pcl}(V)^\infty(\mathbb{F}_q)| - p_{n-m-1} &\leq 14D_{\mathbf{L}}^3\delta_{\mathbf{L}}^2q^{n-m-2}. \end{aligned}$$

Arguing as in (4.4) we obtain

$$\begin{aligned} (5.4) \quad |V(\mathbb{F}_q)| - q^{n-m} &\leq |\text{pcl}(V)(\mathbb{F}_q)| - p_{n-m} + |\text{pcl}(V)^\infty(\mathbb{F}_q)| - p_{n-m-1} \\ &\leq (q + 1)14D_{\mathbf{L}}^3\delta_{\mathbf{L}}^2q^{n-m-2} \leq 21D_{\mathbf{L}}^3\delta_{\mathbf{L}}^2q^{n-m-1}. \end{aligned}$$

We are now ready to state the main result of the section.

Theorem 5.4. *For $q > n$ and $m + 2 \leq r \leq n - m$, we have*

$$|\mathcal{A}_{\lambda}| - \mathcal{T}(\lambda)q^{n-m} \leq q^{n-m-1}(21\mathcal{T}(\lambda)D_{\mathbf{L}}^3\delta_{\mathbf{L}}^2 + n(n-1)).$$

Proof. Combining (4.6) and (4.7) with (5.4), we see that

$$\begin{aligned} |\mathcal{A}_{\lambda}| - \mathcal{T}(\lambda)q^{n-m} &\leq \mathcal{T}(\lambda)|V(\mathbb{F}_q)| - q^{n-m} + |\mathcal{A}_{\lambda}^{nsq}| \\ &\leq \mathcal{T}(\lambda)21D_{\mathbf{L}}^3\delta_{\mathbf{L}}^2q^{n-m-1} + |\mathcal{A}_{\lambda}^{nsq}|. \end{aligned}$$

The statement of the theorem follows immediately from (4.8). \square

Finally, we apply Theorem 5.4 to any family consisting of the elements of \mathcal{P} with certain prescribed coefficients. More precisely, let $\mathcal{A}^m := \mathcal{A}^m(\mathcal{I}, \alpha)$ be the family of polynomials of (4.10). For a given factorization pattern λ and the polynomial $G \in \mathbb{F}_q[\mathbf{X}, T]$ of (2.4), by (4.11) we see that $f := G(\mathbf{x}, T)$ belongs to \mathcal{A}_{λ}^m if and only if there exists \mathbf{x} of type λ with $(-1)^{i_j}\Pi_{i_j}(\mathbf{Y}(\mathbf{x})) = \alpha_{i_j}$ for $1 \leq j \leq m$.

If $\delta_{\mathcal{I}} := i_1 \cdots i_m$ and $D_{\mathcal{I}} := \sum_{j=1}^m (i_j - 1)$, then by Theorem 5.4 we obtain the following result.

Corollary 5.5. *If $q > n$ and $i_m \leq n - m - 2$, then we have*

$$||\mathcal{A}_{\lambda}^m| - \mathcal{T}(\lambda) q^{n-m}| \leq q^{n-m-1} (21 \mathcal{T}(\lambda) D_{\mathcal{I}}^3 \delta_{\mathcal{I}}^2 + n(n-1)).$$

Comparing the estimates of Theorems 4.2 and 5.4, we observe that the latter shows that $|\mathcal{A}_{\lambda}| = \mathcal{T}(\lambda) q^{n-m} + \mathcal{O}(q^{n-m-1})$, while the former only asserts that $|\mathcal{A}_{\lambda}| = \mathcal{T}(\lambda) q^{n-m} + \mathcal{O}(q^{n-m-1/2})$. Indeed, for $q \geq (11D_{\mathcal{I}}^2 \delta_{\mathcal{I}})^2$ the upper bound for $||\mathcal{A}_{\lambda}| - \mathcal{T}(\lambda) q^{n-m}|$ of Theorem 5.4 is smaller than that of Theorem 4.2. Furthermore, Theorem 5.4 holds without any restriction on the characteristic p of \mathbb{F}_q , while Theorem 4.2 is valid only for $p > 2$. On the other hand, Theorem 4.2 allows a larger range of values of m , namely $1 \leq m \leq n - 3$, while Theorem 5.4 requires that $1 \leq m \leq n/2 - 1$. We may summarize these remarks by saying that both results are somewhat complementary.

REFERENCES

- [CGH91] L. Caniglia, A. Galligo, and J. Heintz. Equations for the projective closure and effective Nullstellensatz. *Discrete Appl. Math.*, 33:11–23, 1991.
- [CM06] A. Cafure and G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields Appl.*, 12(2):155–185, 2006.
- [CM07] A. Cafure and G. Matera. An effective Bertini theorem and the number of rational points of a normal complete intersection over a finite field. *Acta Arith.*, 130(1):19–35, 2007.
- [CMP12a] A. Cafure, G. Matera, and M. Privitelli. Polar varieties, Bertini’s theorems and number of points of singular complete intersections over a finite field. Preprint [arXiv:1209.4938 \[math.AG\]](#), 2012.
- [CMP12b] A. Cafure, G. Matera, and M. Privitelli. Singularities of symmetric hypersurfaces and Reed-Solomon codes. *Adv. Math. Commun.*, 6(1):69–94, 2012.
- [CMPP14] E. Cesaratto, G. Matera, M. Pérez, and M. Privitelli. On the value set of small families of polynomials over a finite field, I. *J. Combin. Theory Ser. A*, 124(4):203–227, 2014.
- [Coh70] S. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.
- [Coh72] S. Cohen. Uniform distribution of polynomials over finite fields. *J. Lond. Math. Soc. (2)*, 6(1):93–102, 1972.
- [CvM92] Z. Chatzidakis, L. van den Dries, and A. Macintyre. Definable sets over finite fields. *J. Reine Angew. Math.*, 427:107–135, 1992.
- [Dan94] V. Danilov. Algebraic varieties and schemes. In I.R. Shafarevich, editor, *Algebraic Geometry I*, volume 23 of *Encyclopaedia of Mathematical Sciences*, pages 167–307. Springer, Berlin Heidelberg New York, 1994.
- [Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Grad. Texts in Math.* Springer, New York, 1995.
- [FHJ94] M. Fried, D. Haran, and M. Jarden. Effective counting of the points of definable sets over finite fields. *Israel J. Math.*, 85(1-3):103–133, 1994.
- [FS84] M. Fried and J. Smith. Irreducible discriminant components of coefficient spaces. *Acta Arith.*, 44(1):59–72, 1984.
- [Ful84] W. Fulton. *Intersection Theory*. Springer, Berlin Heidelberg New York, 1984.
- [GHP99] S. Gao, J. Howell, and D. Panario. Irreducible polynomials of given forms. In *Finite fields: theory, applications, and algorithms. Fourth international conference, Waterloo, Ontario, Canada, August 12–15, 1997*, pages 43–54. Amer. Math. Soc., Providence, RI, 1999.
- [GL02] S. Ghorpade and G. Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Mosc. Math. J.*, 2(3):589–631, 2002.
- [Har92] J. Harris. *Algebraic Geometry: a first course*, volume 133 of *Grad. Texts in Math.* Springer, New York Berlin Heidelberg, 1992.

- [Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.
- [Kun85] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, Boston, 1985.
- [MPP13] G. Matera, M. Pérez, and M. Privitelli. On the value set of small families of polynomials over a finite field, II. Preprint [arXiv:1310.3293 \[math.NT\]](#), to appear in *Acta Arith.*, 2013.
- [Sha94] I.R. Shafarevich. *Basic Algebraic Geometry: Varieties in Projective Space*. Springer, Berlin Heidelberg New York, 1994.
- [Ste87] S. Stepanov. The number of irreducible polynomials of a given form over a finite field. *Math. Notes*, 41:165–169, 1987.
- [Vog84] W. Vogel. *Results on Bézout’s theorem*, volume 74 of *Tata Inst. Fundam. Res. Lect. Math.* Tata Inst. Fund. Res., Bombay, 1984.

¹INSTITUTO DEL DESARROLLO HUMANO, UNIVERSIDAD NACIONAL DE GENERAL SARMIENTO, J.M. GUTIÉRREZ 1150 (B1613GSX) LOS POLVORINES, BUENOS AIRES, ARGENTINA
E-mail address: {ecesarat, gmatera, vperez}@ungs.edu.ar

² NATIONAL COUNCIL OF SCIENCE AND TECHNOLOGY (CONICET), ARGENTINA